THESE

Mathématiques

Abderrahmane Nitaj

Conséquences et aspects expérimentaux des conjectures abc et de Szpiro.

Caen (France), 1994 :

YVES HELLEGOUARCH, DIRECTEUR, CAEN,

MICHEL LANGEVIN, RAPPORTEUR, LILLE,

JOSEPH OESTERLÉ, RAPPORTEUR, PARIS,

ERIC REYSSAT, CAEN,

BRIGITTE VALLÉE, CAEN.

A B C

Table de matières

PRESENTATION

Ce travail a pour but l'étude, aussi bien théorique qu'expérimentale de deux conjectures contemporaines. La première est la conjecture, ou plus exactement les conjectures de Szpiro et la deuxième est la conjecture d'Oesterlé-Masser, connue aussi sous le nom de conjecture *abc*.

Les conjectures de Szpiro étudient le lien entre le discriminant minimal des courbes elliptiques et entre leur conducteurs. Dans le cas particulier des courbes elliptiques semi-stables, ce conducteur est précisement le produit des facteurs premiers composant le discriminant minimal.

La conjecture *abc* (dans $\mathbb{Z}$) étudie quant à elle le lien entre la plus grande valeur absolue de trois entiers non nuls premiers entre eux et de somme nulle et entre le produit des facteurs premiers composant ces nombres. Cette conjecture implique entre autre que l'un des trois entiers en question est mal composé, c'est-à-dire qu'il n'est pas très grand relativement au produit des nombres premiers le composant.

Ce travail est composé de deux parties principales. La première partie est théorique et étudie les conjectures de Szpiro ainsi que la conjecture *abc* et de leur importance en Théorie des Nombres. La deuxième partie étudie les aspects expérimentaux, ainsi que des moyens permettant d'obtenir de bons résultats numériques allant curieusement dans le sens contraire de ces conjectures. Sans pour autant prouver ou infirmer ces conjectures, ces exemples sont cependant presque des contres exemples, et leur nombre est curieusement élevé.

Le premier chapitre commence par une description des conjectures de Szpiro, puis la description de la conjecture *abc*. Le lien entre ces conjectures est clairement établi. Ce chapitre théoriques est consacré essentiellement ensuite aux conséquences de ces conjectures en Théorie des Nombres. On montre ainsi que plusieurs conjectures et questions ouvertes peuvent être résolues si la conjecure *abc* est prouvée. On montre par exemple que les conjectures de Fermat, d'Erdös-Woods, de Hall, de Catalan, de Pillai, de Shorey-Tijdeman, de Mollin-Walsh, de Calderbank, d'Erdös-Stewart et d'autres ne portant pas spécialement de noms sont des conséquences totales ou partielles de la conjecture *abc*. On montre aussi comment les conjectures de Szpiro et la conjecture *abc* interviennent dans certains problèmes non résolus, comme par exemple le critère de Wieferich, le problème de Brocard, le problème d'Edgar, le problème de Goormaghtigh et d'autres en les résolvant totalement ou partiellement. Une conséquence importante de la conjecture *abc* particulièrement est le traîtement des équations diophantienes, en montrant généralement que leur nombre de solutions est fini. C'est le cas par exemples des équations diophantiennes suivantes, sous certaines conditions supplémentaires portant souvent sur les exposants:

$$x^n + y^n = z^n \quad \text{en entiers } x, y, z, n,$$
$$x^3 - y^2 = k, \quad \text{en entiers } x, y,$$
$$ax^m - by^n = c, \quad \text{en entiers } x, y, m, n,$$
$$ax^l + by^m = cz^n \quad \text{en entiers } x, y, z, l, m, n,$$
$$n! + 1 = y^2 \quad \text{en entiers } n, y,$$
$$x^n + y^n = n!z^n \quad \text{en entiers } x, y, z, n,$$
$$1 + x + \cdots + x^{n-1} = y^k \quad \text{en entiers } x, y, n, k.$$

Le deuxième chapitre constitue un lien entre la partie théorique et la partie pratique. Il traîte des équations de Thue, de l'algorithme de Cornacchia et des équations de Pell.

On détermine pour l'équation de Thue une borne inférieure pour les solutions ne dépendant que du polynôme intervenant dans cette équation pour que les solutions proviennent du développement en fractions continues de certains nombres réels, dépendant de l'équation. L'algorithme de Cornacchia est révisé, simplifié et étudié de point de vue algorithmique. L'équation de Pell est étudiée plus en détail, aussi bien de point de vue théorique qu'algorithmique. Un algorithme est établi pour la résolution de ces équations. On établit ensuite la complexité des algorithmes de Cornacchia et de celui permettant de résoudre les équations de Pell. Comme première application des équations de Thue, on étudie le quotient de Szpiro pour certaines familles de courbes elliptiques semi-stables, déterminant ainsi plusieurs "presque contre exemples" pour la conjecture de Szpiro sur les courbes elliptiques. Une deuxième application des équations de Thue est la recherche des nombres de Ramanujan. Ce sont des entiers positifs n qui s'écrivent d'au moins deux façons différentes sous la formes $n = x_1^3 + y_1^3 = x_2^3 + y_2^3$.

Le troisième chapitre décrit un algorithme de recherche de bons exemples pour le conjecture *abc* et pour la conjecture de Szpiro relative aux relations *abc*, et qui sont des triplets (a, b, c) d'entiers premiers entre eux et tels que $a+b+c=0$. Cet algorithme utilise la résolution des congruences, l'utilisation des méthodes d'approximations et la factorisation des entiers. On étudie aussi les moyens de le rendre plus efficace, en jouant par exemple sur la nature des paramètres

Le quatrième chapitre traîte des aspects expérimentaux des conjectures de Spiro et de la conjecture *abc*. On étudie en particulier les quotients de Szpiro pour les relations *abc*, ainsi que le quotient d'Oesterlé-Masser. Il présente enfin la liste des meilleurs exemples numériques relativement aux conjectures de Szpiro et à la conjecture *abc*. Ces exemples sont listés en tables indiquant leur importance décroissante pour ces conjectures.

CHAPITRE 1

Les conjectures de Szpiro et de Oesterlé-Masser

Les conjectures de Szpiro et de Oesterlé-Masser

I. Les relations abc

Définition 1. *Une relation abc est une relation de la forme $a+b+c=0$ où a, b et c sont des entiers premiers entre eux.*

Les relations *abc* jouent un rôle fondamental en théorie des nombres. Nous allons citer quelques unes de ces relations.
Quelle plus belle relation peut-on rêver qu'une relation de Fermat:

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

où $n \geq 3$ et $xyz \neq 0$? On savait depuis longtemps (Voir [Rib1], p.164) qu'on ne pouvait pas avoir de telles relations pour $3 \leq n \leq 10^6$. Cette borne a été portée récemment 4×10^6 (voir [B-C-E-M]). En juin 1993, A. Wiles a surpris le monde mathématique en annonçant la résolution du théorème de Fermat. Malheureusement, sa démonstration n'est pas jugée encore complète. Aujourd'hui encore, la conjecture de Fermat reste non démontrée.
Sont célèbres aussi les triplets de Pythagore $(m^2+n^2, m^2-n^2, 2mn)$ qui vérifient la relation *abc*:

$$(m^2+n^2)^2 = (m^2-n^2)^2 + 2^2m^2n^2,$$

où m et n sont des entiers non nuls, premiers entre eux et de parités différentes.
Certaines égalités spéciales de la théorie des nombres forment aussi des relations *abc*. Nous en énumérons quelques unes.
- La relation de définition des nombres de Fermat $F_n = 2^{2^n} + 1$, que celui-ci croyait tous premiers, ce qui est vrai pour $n = 0, 1, 2, 3, 4$, mais faux pour $5 \leq n \leq 21$ et pour d'autres valeurs de n, fournit des relations *abc*. On conjecture actuellement que seul un nombre fini de nombres de Fermat sont premiers.
- La relation de définition des nombres de Mersenne $M_p = 2^p - 1$, où p est un nombre premier. On conjecture par contre qu'il y a une infinité de nombres de Mersenne premiers.
- Le (petit) théorème de Fermat montre que pour tout nombre premier p, les relations $a^{p-1} \equiv 1 \pmod{p}$ sont réalisées pour tout entier a premier avec p: ceci donne autant de relations *abc*.

- Un autre théorème célèbre est le théorème de Wilson qui établit que tout nombre premier p vérifie $(p-1)! \equiv -1 \pmod{p}$. Ces congruences fournissent aussi des relations abc. Les nombres premiers p vérifiant $(p-1)! \equiv -1 \pmod{p^2}$ sont appelés les nombres de Wilson.
- La généralisation du (petit) théorème de Fermat donne aussi des relations abc: pour tous entiers m et a premiers entre eux, $a^{\phi(m)} \equiv 1 \pmod{m}$, où ϕ désigne la fonction d'Euler.
- Les nombres de Wieferich sont des nombres premiers vérifiant $2^{p-1} \equiv 1 \pmod{p^2}$. Leur finitude est encore une question ouverte. Nous verrons plus loin que la conjecture abc implique qu'il y a une infinité de nombres premiers qui ne sont pas des nombres de Wieferich.
- Les nombres de Poulet (ou pseudopremiers en base 2) sont des nombres entiers composés n tels que $2^{n-1} \equiv 1 \pmod{n}$. Les nombres de Poulet sont en nombre infini (voir [Niv-Zuk-Mon]).
- Les nombres de Carmichael sont les entiers composés n tels que $a^{n-1} \equiv 1 \pmod{n}$ pour tout entier a, $1 < a < n$ tel que $(a,n) = 1$. L'existence d'une infinité de nombres de Carmichael a été démontré en 1992 par C. Pomerance.

Toutes ces relations abc, qui au départ sont indépendantes entre elles, entrent dans le cadre d'une grande conjecture contemporaine: la conjecture abc. Nous verrons au long de ce chapitre dans quelle mesure cette conjecture peut donner des informations sur ces relations.

Nous allons définir une fonction qui interviendra constamment dans la suite et qui est en fait liée à la conjecture abc.

Définition 2. *Soit n un entier non nul. On appelle radical de n et on écrit $r(n)$ le produit*

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

des facteurs premiers divisant n. Le radical de n est aussi appelé son support ou son conducteur.

II. Les conjectures de Szpiro

1. Enoncés.

Soit E une courbe elliptique définie sur $\mathbb{Q}$, de discriminant minimal Δ_E et de conducteur N_E (voir Appendice A). Lorsque E est semi-stable, alors $N_E = r(|\Delta_E|)$.
Nous allons commmencer en énonçant trois conjectures de Szpiro.

Conjecture 1. (Szpiro, forme forte). *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que l'on ait:*

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

pour toute courbe elliptique semi-stable E sur $\mathbb{Q}$, de discriminant minimal Δ_E et de conducteur N_E.

Nous allons utiliser une démonstration d'Oesterlé [Oes] pour montrer que la condition $\varepsilon > 0$ est nécessaire dans cette conjecture.

Proposition 1. *Soit $\varepsilon \longmapsto c(\varepsilon)$ une application vérifiant la conjecture 1. Alors*

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

Preuve. Définissons les trois suites (a_n), (b_n) et (c_n) par $a_0 = 16$, $b_0 = 1$, $c_0 = -17$ et:

$$\begin{aligned} a_{n+1} &= 4a_n b_n, \\ b_{n+1} &= (a_n - b_n)^2, \\ c_{n+1} &= -(a_n + b_n)^2. \end{aligned}$$

Ces suites vérifient pour tout $n \geq 0$, $c_n \equiv -1 \pmod 4$, $16|a_n$ et $a_n + b_n + c_n = 0$. On peut vérifier facilement que $(a_n, b_n) = 1$. Considérons la courbe elliptique E_n définie sur $\mathbb{Q}$ par la forme de Weiersrass:

$$E_n : \ y^2 + xy = x^3 + \frac{a_n - c_n - 1}{4} x^2 - \frac{a_n c_n}{16} x.$$

Comme nous le verrons dans la partie II, proposition 3, cette courbe est semi-stable sur $\mathbb{Q}$ et le modèle donné ci-dessus est minimal. Son discriminant minimal est

$$\Delta = \left(\frac{a_n b_n c_n}{16} \right)^2.$$

Appliquons la conjecture 1 à cette courbe. Nous obtenons:

$$\left(\frac{a_n b_n c_n}{16} \right)^2 \leq c(\varepsilon) \left(r \left(\frac{a_n b_n c_n}{16} \right) \right)^{6+\varepsilon},$$

ce qui donne:

$$c(\varepsilon) \geq \frac{(a_n b_n c_n/16)^2}{(r(a_n b_n c_n/16))^{6+\varepsilon}}.$$

Posons

$$\lambda_n = \frac{(a_n b_n c_n/16)^2}{(r(a_n b_n c_n/16))^6}.$$

Pour $n \geq 1$, on a $2^6 | a_n$ et donc $r(4a_n/16) = r(a_n/16)$. Alors:

$$\underline{\lim}_{\varepsilon \to 0} c(\varepsilon) \geq \lambda_{n+1} \geq 16\lambda_n \frac{(a_n + b_n)^2}{(a_n - b_n)^2} > 16\lambda_n.$$

Ceci implique donc que $\lim_{\varepsilon \to 0} c(\varepsilon) = +\infty$. ■

Il existe aussi une conjecture de Szpiro, dite "faible" qui s'énonce ainsi:

Conjecture 2. (Szpiro, forme faible). *Il existe deux constantes absolues c_1 et c_2 telles que pour toute courbe elliptique semi-stable sur $\mathbb{Q}$, de discriminant minimal Δ_E et de conducteur N_E on ait:*

$$|\Delta_E| \leq c_1 N_E^{c_2}.$$

Nous allons suivre S. Lang pour énoncer la conjecture suivante(voir [Lan]):

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

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

Nous allons montrer maintenant quel est le lien entre les conjectures 1 et 3.

Proposition 2. *La conjecture 3 implique la conjecture 1.*

Preuve. Soit E une courbe elliptique semi-stable définie sur $\mathbb{Q}$ par un modèle minimal. Les quantités Δ_E, c_4 et c_6 liées à cette courbe vérifient:

$$\begin{cases} \Delta_E, c_4, c_6 \text{ entiers}, \\ (c_4, \Delta_E) = (c_6, \Delta_E) = 1, \\ c_4^3 - c_6^2 = 1728\Delta_E. \end{cases}$$

Puisque E est semi-stable, alors son conducteur vérifie $N_E = r(\Delta_E)$. Admettons la conjecture 3 et appliquons-la au triplet $(1728\Delta_E, -c_4^3, c_6^2)$, on obtient:

$$|c_4| \leq c_1(\varepsilon) N_E^{2+\varepsilon} \qquad \text{et} \qquad |c_6| \leq c_1(\varepsilon) N_E^{3+\varepsilon},$$

d'où l'on tire:

$$|1728\Delta_E| \le |c_4|^3 + c_6^2 \le c_2(\varepsilon) N_E^{6+3\varepsilon},$$

ce qui donne ensuite l'inégalité de la conjecture 1. ■

2. Les quotients de Szpiro.

(a) Cas général. Pour une courbe elliptique semi-stable définie sur $\mathbb{Q}$, de discriminant minimal Δ_E et de conducteur $N_E = r(\Delta_E)$, la conjecture 1 implique que

$$\log |\Delta_E| \le \log c(\varepsilon) + (6+\varepsilon) \log N_E,$$

et donc que le rapport

$$\sigma_E = \frac{\log |\Delta_E|}{\log N_E}$$

est borné. Ce rapport est appelé quotient de Szpiro pour les courbes elliptiques semi-stables. Nous donnerons dans le chapitre 2 des exemples de courbes elliptiques semi-stables sur $\mathbb{Q}$ ayant un quotient de Szpiro assez élevé par rapport à la valeur conjecturale 6. Comme on l'a vu dans la proposition 1, il existe un nombre infini de courbes elliptiques semi-stables sur $\mathbb{Q}$ pour lesquelles le quotient de Szpiro est supérieur à 6. Dans [Fo-Na-Te], en utilisant des outils analytiques, E. Fouvry, M. Nair et G. Tenenbaum ont montré que pour tout $\varepsilon > 0$, l'ensemble des classes des courbes elliptiques semi-stables pour les quelles $\sigma_E > 1+\varepsilon$ est négligeable dans l'ensemble des classes des courbes elliptiques semi-stables.

(b) Courbes elliptiques E_{abc}. Soient a, b, c des entiers premiers entre eux vérifiant $a+b+c=0$. Soit E_{abc} la courbe elliptique définie sur $\mathbb{Q}$ par l'équation:

$$E_{abc} : Y^2 = X(X-a)(X+b). \tag{1}$$

Ces courbes ont été introduites par Y. Hellegouarch en 1972 dans [Hel1], pour l'étude de l'équation de Fermat:

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

en entiers x, y, z tels que $xyz \neq 0$ où $n \ge 3$ est donné. Elles ont été utilisées ensuite par G. Frey pour étudier le lien entre les courbes elliptiques et les triplets (a, b, c) tels que $a+b+c=0$, (voir [Fre]). Le discriminant du modèle de Weierstrass de la courbe E_{abc} est $\Delta = 16(abc)^2$ et l'invariant c_4 est $c_4 = -16(ab+ac+bc)$. La quantité $ab+ac+bc$ est toujours impaire puisque un seul des entiers a, b ou c est pair, et donc le modèle (1) est minimal en 2. Si $abc \not\equiv 0 \pmod{16}$, alors $(\Delta, c_4) = 16$ et le modèle (1) n'est pas un modèle minimal semi-stable en 2. Si $16|abc$, alors l'un des trois entiers a, b ou c est de la forme $4n-1$ avec $n \in \mathbb{Z}$. Supposons par exemple que a, b et c vérifient le système:

$$
(2) \qquad \begin{cases} a+b+c=0, \\ a \equiv -1 \pmod 4, \\ 16|b. \end{cases}
$$

En effectuant le changement de variables $X=4x$ et $Y=8y+4x$, on obtient une nouvelle équation pour la courbe E_{abc}:

$$
(3) \qquad E_{abc} : y^2 + xy = x^3 + \frac{b-a-1}{4}x^2 - \frac{ab}{16}x.
$$

Proposition 3. *Si a, b et c vérifient le système (2), alors l'équation (3) est un modèle minimal sur $\mathbb{Z}$ et représente une courbe elliptique semi-stable.*

Preuve. Puisque les entiers a, b et c vérifient le système (2), alors $\frac{b-a-1}{4}$ et $\frac{ab}{16}$ sont des entiers. Les invariants Δ et c_4 sont:

$$
\Delta = \left(\frac{abc}{16}\right)^2 \qquad \text{et} \qquad c_4 = -(ab+bc+ca).
$$

Or $c_4 = c^2 - ab$ et donc $(\Delta, c_4) = 1$. Alors, (voir Appendice A) l'équation (3) représente un modèle minimal et la courbe E_{abc} est semi-stable. ■

On donne maintenant la conjecture suivante relative aux triplets abc.

Conjecture 4. (Szpiro pour les relations abc). *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout triplet d'entiers premiers entre eux vérifiant $a+b+c=0$ et $16|abc$ on ait:*

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

On a alors la proposition suivante.

Proposition 4. *La conjecture 1 implique la conjecture 4.*

Preuve. Si a, b et c vérifient le sytème (2), alors la conjecture 1 appliquée à la courbe elliptique E_{abc} définie par (3) donne:

$$
\left(\frac{abc}{16}\right)^2 \leq c(\varepsilon)\left(r\left(\frac{abc}{16}\right)\right)^{6+\varepsilon} \leq c(\varepsilon)\,(r(abc))^{6+\varepsilon}
$$

et donc:

$$|abc| \leq 2^4 c(\varepsilon))^{1/2} \left(r(abc)\right)^{3+\varepsilon/2},$$

d'où la conclusion de la conjecture 4. ■

Remarque. L'inégalité de la conjecture 4 peut être étendue aux relations abc même si $16 \not| abc$, car si $a+b=c$, alors l'un des trois entiers a, b ou c est pair. On suppose par exemple que b est pair. En appliquant la conjecture 4 à la relation: $(a^2+b^2)^2 = (a-b)^2(a+b)^2 + 4a^2b^2$, on obtient l'inégalité $|abc| \leq c(\varepsilon)\left(r(abc)\right)^{3+\varepsilon}$. Ceci se fait par une méthode analogue à la démonstration de la proposition 1.

L'inégalité de la conjecture 4 implique que le rapport

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

est borné. Nous l'appellerons rapport de Szpiro pour les relations abc. Nous expliciterons dans le chapitre 4 plusieurs familles infinies de triplets abc pour lesquels on a $\rho(a,b,c) > 3$.

Nous donnons enfin une dernière conjecture de Szpiro, qui est en fait une conséquence de la conjecture 1. En quotientant la courbe elliptique E_{abc} définie par (1) par ses sous groupes d'ordre deux, on obtient trois courbes elliptiques semi-stables de discriminants minimaux $-a^4bc/16$, $-a(b/16)^4c$ et $-abc^4/16$ et de conducteurs communs $r(abc/16)$. En appliquant la conjecture 1 à ces courbes, on obtient, la conjecture suivante, valable d'abord sous les conditions (2), mais qu'on peut étendre ensuite à tout triplet (a,b,c) d'entiers premiers entre eux en utilisant la remarque ci-dessus (voir aussi [Szp] et [Oes]).

Conjecture 5. *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout triplet (a,b,c) d'entiers premiers entre eux vérifiant $a+b+c=0$ on ait:*

$$\max(|a|,|b|,|c|) \leq c(\varepsilon)\left(r(abc)\right)^{6/5+\varepsilon}.$$

III. La conjecture abc

Motivés par un théorème de Mason sur les polynômes et par les conjectures de Szpiro décrites ci-dessus, J. Oesterlé et D.W. Masser ont formulé en 1985 la conjecture suivante:

Conjecture 6. (abc, Oesterlé-Masser). *Soit $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout triplet (a,b,c) d'entiers, premiers entre eux vérifiant $0 < a < b < c$ et $a+b=c$ on ait:*

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

Cette conjecture est née à Bonn d'une discution entre J. Oesterlé et D. W. Masser. Oesterlé avait posé la question sur la possibilité de trouver le meilleur exposant espérable α tel que pour tout triplet (a, b, c) d'entiers strictement postifs, premiers entre eux et vérifiant $a + b = c$ on ait:

$$c < (r(abc))^{\alpha} .$$

Par analogie avec le théorème de Mason, Oesterlé et Masser ont suggéré la forme donnée dans la conjecture 6.
Une forme équivalente de la conjecture abc est donnée par la proposition suivante:

Proposition 5. *La conjecture abc est telle que pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout triplet (a, b, c) d'entiers, premiers entre eux et vérifiant $a+b+c = 0$ on ait:*

$$r(abc) \geq c(\varepsilon) (\max(|a|, |b|, |c|))^{1-\varepsilon} .$$

Preuve. Ceci provient tout simplement du fait que pour tous réels positifs A et B, l'inégalité:

$$A \leq c_1(\varepsilon) B^{1+\varepsilon},$$

est équivalente à:

$$B \geq \left(\frac{A}{c_1(\varepsilon)}\right)^{1/(1+\varepsilon)} = c_2(\varepsilon') A^{1-\varepsilon'},$$

avec $\varepsilon' = \varepsilon/(1 + \varepsilon)$. ∎

Une première analyse de l'inégalté de la conjecture abc montre que le produit abc contient un grand nombre de facteurs premiers ou qu'il contient quelques grands facteurs premiers avec des exposants relativement petits. On peut le vérifier sur les quelques exemples numériques de la table 1 ci-dessous où $a_n = 1$, $b_n = 5^{2^n} - 1$ et $c_n = 5^{2^n}$ pour $3 \leq n \leq 7$. Ces exemples sont plutôt optimistes pour l'inégalité de la conjecture abc car $2^{n+2} | 5^{2^n} - 1$.

Table 1

n	a	b	c
3	1	$2^5.3.13.313$	5^{2^3}
4	1	$\left(5^{2^3} - 1\right).2.17.11489$	5^{2^4}
5	1	$\left(5^{2^4} - 1\right).2.2593.29423041$	5^{2^5}
6	1	$\left(5^{2^5} - 1\right).2.641.75068993.241931001601$	5^{2^6}
7	1	$\left(5^{2^6} - 1\right).2.769.3666499598977.9613295678264374195l225664001$	5^{2^7}

On peut aussi constater le même phénomène dans les tables de factorisation de nombres de la forme $a^n - b^n$ données à la fin du livre de H. Riesel (voir [Rie], pp 381-437).
La proposition suivante montre que le choix de $\varepsilon = 0$ n'est pas possible dans la conjecture *abc*.

Proposition 6. *Soit $\varepsilon \longmapsto c(\varepsilon)$ une application vérifiant la conjecture abc. Alors*

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

Cette proposition est un corollaire de la proposition 1. Une autre démonstration se trouve dans [Lan]. Nous donnons malgré tout une autre démonstration, qui se distingue particulièrement par sa simplicité.

Preuve. La relation évidente $3^2 - 2^3 = 1$ nous donne une infinité de couples d'entiers (x_n, y_n) premiers entre eux, vérifiant pour tout $n \geq 1$, $x_n^2 - 2y_n^2 = 1$. En effet, soient $x_1 = 3$ et $y_1 = 2$. Pour tout $n \geq 1$, on définit les entiers x_n et y_n par la relation:

$$x_n + y_n\sqrt{2} = \left(x_1 + y_1\sqrt{2}\right)^n.$$

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 $c(\varepsilon) \geq 2^{m(1+\varepsilon)} / x_n^{2\varepsilon}$. d'où

$$\underline{\lim}_{\varepsilon \to 0} c(\varepsilon) \geq 2^m,$$

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

Nous donnerons une autre démonstration de la proposition 6 dans le chapitre 4 en exhibant plusieurs familles infinies de triplets *abc* (x, y, z) avec $0 < x < y$ pour lesquels le rapport de Oestrlé-Masser:

$$\alpha = \alpha(x, y, z) = \frac{\log z}{\log r(xyz)},$$

est supérieur à la valeur conjecturale 1. Enfin, une autre démonstration de la proposition 6 résulte d'un travail de C. L. Stewart et R. Tijdeman (voir [Ste-Tij]) qui ont établit le théorème suivant:

Théorème 1. (Stewart, Tijdeman, 1986). *Pour tout $\varepsilon > 0$, il existe une infinité de triplets (a,b,c) d'entiers positifs verifiant $(a,b,c) = 1$, $a+b=c$ et*

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

Dans leur démonstration, Stewart et Tijdeman ont seulement prouvé l'existence de tels triplets. Soit $\varepsilon > 0$ donné. Si (a,b,c) est un triplet qui vérifie l'inégalité du théorème 1, alors:

$$\varepsilon > 4 - (\log c - \log r)\,\frac{\log\log r}{\sqrt{\log r}} = \tau(a,b,c) = \tau.$$

Il suffit donc que le triplet (a,b,c) vérifie $\tau \leq 0$. Ces triplets étant nombreux, nous avons regroupé dans la table 2 ci-dessous quelques uns d'entre eux avec $\tau < -2$.

Table 2

a	b	c	τ
$3^{13}.5^4.23.73^3$	$2^{24}.13^{12}$	$11^{12}.29.4294769$	-3.83134
$151^2.7^4.181^4$	$2^{25}.29.3^4.10753$	5^{24}	-3.64801
$2^5.3^{18}$	$5^6.7^{10}.23^2$	$11^9.990203$	-2.90520
$3.31.773^2$	$113^3.5^8.11^4.103^2$	$2.19^{11}.613^2$	-2.81387
61^4	$2^{20}.41^3.83^2$	$3^{22}.5.19.167$	-2.58932
$2^{13}.3^{13}.11^3$	$13.29.43^6.673$	$5^{20}.17$	-2.56459
$7^3.103.2887403261$	$2^7.5^{25}$	$3^{25}.19^6$	-2.27466
$3^2.233$	$23^7.293^2$	$2^{15}.5^2.13^5.31^2$	-2.27108
$2^{33}.5$	$3^9.7^6.31^2.97$	$11^2.19^3.127^4$	-2.16099
$2^{10}.19^{10}$	$5^6.13^4.29^5$	$3^{20}.4425749$	-2.12318
$3^6.157^3.283$	23^{10}	$2^{30}.5^2.11^2.13$	-2.03526

Comme nous l'avons dit au début de cette partie, la conjecture abc dérive en partie des conjectures de Szpiro, on va montrer maintenant quel est le lien entre elles.

Proposition 7. *La conjecture abc est équivalente à la conjecture de Szpiro généralisée.*

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

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

Supposons que $|Au^3| \leq |Bv^2|$, alors $|u| \leq c_3(A,B)|v|^{2/3}$. En portant 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:

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

Supposons que $1 - 5\varepsilon > 0$, alors on obtient:

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

Posons $\varepsilon' = 18\varepsilon/(1-5\varepsilon)$, alors l'inégalité précédente devient:

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

On obtient alors pour $|u|$:

$$|u| \leq c_5^{2/3}(\varepsilon', A, B) c_3(A,B) r(k)^{2(3+\varepsilon')/3} \leq c_6(\varepsilon', A, B) \left(r(k)\right)^{2+\varepsilon'}.$$

Ceci prouve la conjecture de Szpiro généralisée.
2) Inversement, admettons la conjecture de Szpiro généralisée. Reprenons la courbe elliptique E_{abc} définie par l'équation (1), où a, b et c vérifient $(a,b,c) = 1$, $0 < a < b < c$ et $a + b = c$. Son discriminant est $\Delta = 16(abc)^2$ et deux de ses invariants sont $c_4 = 16(a^2+ab+b^2)$ et $c_6 = -32(b-a)(a+2b)(2a+b)$. En simplifiant la relation $c_4^3 - c_6^2 = 1728\Delta$, nous obtenons:

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

Cette relation peut éventuellement être simplifiée par 3^3 si $a \equiv b \equiv 1 \pmod 3$. En appliquant la conjecture de Szpiro généralisée, 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:

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

Ceci prouve la conjecture *abc*. ■

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. 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 [Ste-Tij] et [Ste-Yu] respectivement.

Théorème 2. (Stewart, Tijdeman, 1986**).** *Il existe une constante effectivement calculable $k > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs, vérifiant $(a, b, c) = 1$ et $a + b = c$, on ait:*

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

Théorème 3. (Stewart, Yu, 1990**).** *Il existe une constante effectivement calculable $k > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs, vérifiant $(a, b, c) = 1$ et $a+b = c$, on ait:*

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

Il est clair que le théorème 3 améliore le théorème 2. Les inégalités dans ces deux théorèmes sont exponentielles en $r(abc)$ alors que celle de la conjecture abc est seulement polynômiale. L'inégalité du théorème 3 implique que:

$$\frac{\log\log c}{\log r(abc)} < \frac{2}{3} + \frac{k}{\log\log r(abc)}.$$

Il est à noter qu'aucun exemple numérique ne contredit l'inégalité ci dessus avec $k = 0$. Ainsi, l'exemple d'E. Reyssat $a = 2$, $b = 3^{10}.109$ et $c = 23^5$ donne:

$$\frac{\log\log c}{\log r(abc)} \simeq 0.28614 < 2/3.$$

Le meilleur exemple connu est certainement $a = 1$, $b = 2.3^7$, $c = 5^4.7$ qui donne:

$$\frac{\log\log c}{\log r(abc)} \simeq 0.39765.$$

IV. Applications conjecturales

Dans cette partie, on étudie quelques conséquences des conjectures de Szpiro et de la conjecture abc. Quelques unes existaient déjà dans la littérature (2, 3, 4, 5 6, 7, 8, 10, 11, 22). Les nouvelles conséquences sont donc les suivantes: 1, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23. Dans ces applications conjecturales, nous citerons surtout la conjecture *abc*. Sauf mention contraire, toutes ces applications sont aussi des conséquences des conjectures de Szpiro.

1. Conséquences sur les triplets *abc*. Comme première application de la conjecture *abc*, nous avons la proposition suivante:

Proposition 8. *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, premiers entre eux et vérifiant $x_1 + x_2 = x_3$, on ait pour $i = 1$, $i = 2$ ou $i = 3$:*

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

Preuve. Supposons que la conjecture *abc* est vraie. Alors pour $i = 1, 2, 3$, on a:

$$x_i \leq c(\varepsilon)\,(r(x_1 x_2 x_3))^{1+\varepsilon},$$

et donc:

$$x_1 x_2 x_3 \leq (c(\varepsilon))^3\,(r(x_1 x_2 x_3))^{3+\varepsilon}.$$

Supposons que pour chaque $i = 1, 2, 3$ on ait:

$$x_i > c(\varepsilon)\,(r(x_i))^{3+\varepsilon}.$$

Alors:

$$x_1 x_2 x_3 > (c(\varepsilon))^3\,(r(x_1 x_2 x_3))^{3+\varepsilon},$$

ce qui contredit la conjecture *abc*. ∎

Nous avons aussi le théorème suivant:

Théorème 4. *Si la conjecture abc est vraie, alors pour tout $\varepsilon > 0$, il existe une constante $c_0(\varepsilon) > 0$ telle que pour tout entier $n \geq 2$ et tout entier $x \geq 2$ on ait:*

$$x^{n-1} \leq c_0(\varepsilon)\,(r(x^n - 1))^{1+\varepsilon}.$$

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

$$x^n \leq c_1(\varepsilon)\,(r(x^n - 1))^{1+\varepsilon}\,x^{1+\varepsilon},$$

et ceci donne:
$$x^{n-1-\varepsilon} = \left(x^{n-1}\right)^{1-\varepsilon/(n-1)} \leq c_1(\varepsilon)\left(r(x^n-1)\right)^{1+\varepsilon}.$$
On a ensuite:
$$x^{n-1} \leq (c_1(\varepsilon))^{(n-1)/(n-1-\varepsilon)}\left(r(x^n-1)\right)^{(n-1)(1+\varepsilon)/(n-1-\varepsilon)}.$$
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. ∎

Une autre conséquence de la conjecture *abc* est la proposition suivante:

Proposition 9. *Soit (x_1, x_2, x_3) un triplet d'entiers positifs, non nécessairement premiers entre eux, vérifiant $x_1 < x_2 < x_3$ et $x_1 + x_2 = x_3$. La conjecture abc implique que, pour $i = 1, 2, 3$:*
$$x_3 \leq c(\varepsilon)\left(x_i r(x_1x_2x_3/x_i)\right)^{1+\varepsilon}.$$

Preuve. Soit $d = (x_1, x_2, x_3)$. Appliquons la conjecture *abc* au triplet $(x_1/d, x_2/d, x_3/d)$. On obtient:
$$x_3/d \leq c(\varepsilon)\left(r(x_1x_2x_3/d^3)\right)^{1+\varepsilon} \leq c(\varepsilon)\left(x_i/d\right)^{1+\varepsilon}\left(r(x_1x_2x_3/x_i)\right)^{1+\varepsilon},$$
ce qui donne la conclusion de la proposition. ∎

2. Les nombres de Wieferich. Un nombre premier p vérifiant la congruence:
$$a^{p-1} \equiv 1 \pmod{p^2}, \tag{4}$$
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 grand théorème de Fermat). En 1910, Mirimanoff a prouvé la même chose avec $a = 3$. Les nombres premiers vérifiant la congruence (4) 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 la congruence (4) avec $a = 3$ et $p \leq 2^{30}$ sont 11 et 1006003. Pour plus d'informations, on peut consulter [Rib3]ou [Mon]. Un problème encore ouvert est la conjecture suivante:

Conjecture 7. *Soit $a \geq 2$. Il existe une infinité de nombres premiers ne vérifiant pas la congruence* (4).

J. H. Silverman a montré que cette conjecture est une conséquence de la conjecture *abc*. Pour cela, on a besoin du lemme suivant:

Lemme 1. *Soient a et n des entiers positifs. Si un nombre premier p est tel que $a^n \equiv 1 \pmod p$ et $a^n \not\equiv 1 \pmod{p^2}$, alors il ne vérifie pas la congruence* (4).

Preuve. Soit d l'ordre de a dans le groupe des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$. On a $a^d = 1 + pq$ et comme $a^n \equiv 1 \pmod p$ et $a^n \not\equiv 1 \pmod{p^2}$, alors $d|n$ et $a^d \not\equiv 1 \pmod{p^2}$ et donc $(p, q) = 1$. Maintenant on a:

$$a^{p-1} = \left(a^d\right)^{(p-1)/d} = (1 + pq)^{(p-1)/d} \equiv 1 + pq(p-1)/d \pmod{p^2},$$

avec $(p, q(p-1)/d) = 1$. Il en résulte que $a^{p-1} \not\equiv 1 \pmod{p^2}$. ■

Proposition 10. (Silverman) *La conjecture abc implique la conjecture 7.*

Preuve. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers ne vérifiant pas la congruence (4). Soit $a \geq 2$ un entier. On peut écrire pour tout entier positif n :

$$a^n - 1 = a_n b_n$$

où a_n est la partie qui contient tous les nombres premiers qui divisent $a^n - 1$ et qui ne vérifient pas (4) et où $b_n = (a^n - 1)/a_n$. Si $p|b_n$, alors p vérifie:

$$a^{p-1} \equiv 1 \pmod{p^2}$$

et par le lemme 1, $p^2|a^n - 1$. Alors $p^2|b_n$ et donc b_n vérifie $r(b_n) \leq b_n^{1/2}$. En appliquant la conjecture *abc* au triplet $(1, a^n - 1, a^n)$ on obtient, sachant que $r(a_n)$ est borné:

$$a_n b_n \leq c_1(\varepsilon)\left(r(aa_n b_n)\right)^{1+\varepsilon} \leq c_2(\varepsilon) b_n^{(1+\varepsilon)/2},$$

et donc:

$$a_n b_n^{(1-\varepsilon)/2} \leq c_2(\varepsilon).$$

Si ε est assez petit, l'inégalité ci-dessus devient impossible pour les grandes valeurs de n, ce qui prouve donc la proposition 10. ■

3. Le théorème de Faltings et la conjecture de Mordell. Une des conséquences les plus étonnantes de la conjecture *abc* est le fait que celle-ci implique tout simplement le théorème de Faltings (ex conjecture de Mordell) sur $\mathbb{Q}$:

Théorème 5. (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 démontrée successivement par G. Faltings, P. Vojta et E. Bombieri. Ces démonstrations sont toutefois assez compliquées contrairement à la démonstration obtenue par N. Elkies en 1991 (voir [Elk]) en supposant vraie la conjecture *abc*:

Théorème 6. (Elkies). *La conjecture abc implique la conjecture de Mordell.*

La preuve de ce théorème a pour point de départ un théorème de Belyi et utilise des propriétés élémentaires des hauteurs des points rationnels des courbes définies sur un corps de nombres. Elkies donne à la fin de son article le corollaire suivant:

Corollaire 1. (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 $c(\varepsilon, P) > 0$ telle que pour tout couple (a,b) d'entiers premiers entre eux, vérifiant $P(a,b) \neq 0$ on ait:*

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

4. Le dernier théorème de Fermat. En 1637, Fermat a énoncé une assertion qui est encore sans preuve. Cette assertion porte le nom de "Grand Théorème de Fermat", mais en fait c'est une conjecture. Pour plus d'informations, on peut consulter par exemple le livre de P. Ribenboim [Rib1]. En juin 1993, A. Wiles surprena les spécialistes de la question en annonçant la résolution de la conjecture de Fermat. Actuellement, cette affirmation n'est pas encore confirmée. Par rapport au travail de Wiles, qui traite le théorème de Fermat dans sa généralité, la proposition suivante ne concerne que le cas asymptotique, et se distingue par sa simplicité, en admettant la conjecture *abc* ou l'une des conjectures de Szpiro.

Proposition 11. *La conjecture abc entraîne le théorème de Fermat pour les grandes valeurs de n.*

Preuve. Supposons qu'il existe des entiers x, y, z et n vérifiant $n \geq 3$, $xyz \neq 0$,$(x,y) = 1$ et

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

En appliquant la conjecture 4 (ou la conjecture abc trois fois) au triplet (a, b, c) defini par $a = x^n$, $b = y^n$ et $c = -z^n$, on obtient:

$$|xyz|^n \leq c(\varepsilon)\left(r(xyz)\right)^{3+\varepsilon} \leq c(\varepsilon)|xyz|^{3+\varepsilon},$$

ce qui donne:

$$(n-3-\varepsilon)\log|xyz| \leq \log c(\varepsilon).$$

Prenons ε tel que $0 < \varepsilon < 1$. Si $n \geq 4$, alors l'inégalité ci-dessus implique d'une part:

$$n-3-\varepsilon \leq \frac{\log c(\varepsilon)}{\log|xyz|} \leq \frac{\log c(\varepsilon)}{\log 6}$$

et donc n est borné. ■

Remarque.
De la dernière inégalité de la proposition ci-dessus, on tire pour les solutions éventuelles de l'équation de Fermat avec $n \geq 4$:

$$\log|xyz| \leq \frac{\log c(\varepsilon)}{n-3-\varepsilon} \leq \frac{\log c(\varepsilon)}{1-\varepsilon},$$

ce qui montre que les solutions sont bornées.
La conjecture 4 implique que pour n assez grand, le problème de Fermat n'a pas de solutions, et que pour les petites valeurs de $n \geq 4$, il n'a qu'un nombre fini de solutions. En comparaison, le théorème de Faltings, entraîne la finitude du nombre de solutions du problème de Fermat pour n fixé, mais ne donne aucune indication sur une limite possible pour n. ■

5. La conjecture d'Erdös-Woods. Commençons d'abord par énoncer cette conjecture.

Conjecture 8. (Erdös-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 implique qu'il existe une constante $k > 0$, telle que le système d'équations diophantiennes

$$r(x+i) = r(y+i), \ \ i = 1, \cdots, k,$$

en entiers positifs x et y n'admet que des solutions vérifiant $x = y$. Il est facile de voir que la constante k ne peut pas être égale à 2, car en prenant $x = 74$ et $y = 1214$, on a $x + 1 = 3 \cdot 5^2$, $y + 1 = 3^5.5$ et $x + 2 = 2^2 \cdot 19$, $y + 2 = 2^6 \cdot 19$.

D'autres contre exemples sont donnés par les couples (x_n, y_n), définis pour tout $n \geq 2$ par:

$$x_n = 2^n - 3,\ y_n = 2^{2n} - 2^{n+1} - 1.$$

Par contre pour $k \geq 3$, aucun exemple d'entiers différents vérifiant les égalités de la conjecture d'Erdös-Woods n'est connu. Un résultat parfaitement établi qui va dans le sens de cette conjecture avec $k \geq 3$ (valable aussi avec $k = 2$) est le suivant.

Théorème 7. *Soit $k \geq 2$ un entier fixé. Pour tout entier positif x, il n'existe au plus qu'un nombre fini d'entiers positifs y vérifiant pour tout i, $1 \leq i \leq k$, $r(x+i) = r(y+i)$.*

Preuve. Soient x et y deux entiers positifs vérifiant les hypothèses du théorème. Posons $x + 1 = p_1^{e_1} \cdots p_r^{e_r}$ où pour tout i, $1 \leq i \leq r$, p_i est un nombre premier et e_i est un entier positif. Alors $y + 1 = p_1^{e_1'} \cdots p_r^{e_r'}$ pour des entiers strictement positifs e_i. Posons de même $x + 2 = q_1^{f_1} \cdots q_s^{f_s}$, alors $y + 2 = q_1^{f_1'} \cdots q_s^{f_s'}$. La relation $(y+2) - (y+1) = 1$ donne:

$$q_1^{f_1'} \cdots q_s^{f_s'} - p_1^{e_1'} \cdots p_r^{e_r'} = 1.$$

Comme x est fixé, les nombres premiers p_i et q_j sont aussi fixés, et l'équation ci-dessus en entiers e_i' et f_j' n'admet qu'un nombre fini de solutions d'après le théorème de Mahler relatif aux équations en S-entiers. ■

Nous allons voir maintenant que la conjecture *abc* permet de répondre positivement à la conjecture d'Erdös-Woods avec $k = 3$, sauf dans un nombre fini de cas. On peut retrouver ce résultat dans [Lange2].

Proposition 12. **(Langevin)** *La conjecture abc implique que la conjecture d'Erdös - Woods est vraie avec $k = 3$, sauf peut être pour un nombre fini d'exceptions pour x et y.*

Preuve. Soient x et y deux entiers strictement positifs. Supposons que $x < y$ et que pour $i = 1, 2, 3$, on ait $r(y+i) = r(x+i) | (x+i)$. Alors $r((y+i)) | (y-x)$. Il en résulte que

$$r((y+1)(y+2)(y+3)) | (y-x).$$

Appliquons la conjecture *abc* à la relation

$$1 + (y+1)(y+3) = (y+2)^2.$$

On obtient:

$$y^2 < (y+2)^2 \leq c(\varepsilon) \left(r((y+1)(y+2)(y+3)) \right)^{1+\varepsilon} \leq c(\varepsilon)(y-x)^{1+\varepsilon} < c(\varepsilon) y^{1+\varepsilon},$$

et donc

$$y^{1-\varepsilon} < c(\varepsilon).$$

Alors pour ε assez petit, ceci implique que y est borné. Autrement dit, pour tout $\varepsilon > 0$, il existe une constante positive $c_0(\varepsilon)$, ne dépendant que de ε telle que si deux entiers x et y vérifient $r(x+i) = r(y+i)$, $i = 1, 2, 3$ et si $y > c_0(\varepsilon)$, alors $x = y$. Ainsi la conjecture d'Erdös-Woods est vraie sauf peut être pour les entiers x et y tels que $x, y \leq c_0(\varepsilon)$. ■

6. La conjecture de Hall. En 1971, M. Hall Jr. a énoncé la conjecture suivante:

Conjecture 9. (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 $(x, y) = (\pm 2, \pm 3)$.
Cette conjecture implique que le rapport

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

ne peut pas être très petit. Dans la table 3, nous avons classé quelques exemples pour lesquels le rapport ci-dessus est assez petit. Ces exemples correspondent à $x \leq 10^{10}$ et $y = [x\sqrt{x}]$ et sont classés par ordre croissant de la dernière colonne.

Table 3

Nr	x	y	$x^3 - y^2$	$\frac{\lvert x^3-y^2\rvert}{\max(x^3,y^2)^{1/6}}$
1	28187351	149651610621	-1090	0.205305
2	5234	378661	-17	0.234981
3	939787	911054064	$+307$	0.316682
4	2	3	-1	0.707107
5	390620082	7720258643465	-14857	0.75171
6	110781386	1166004406095	-8569	0.814136
7	421351	273505487	-618	0.952065
8	93844	28748141	-297	0.969512

Une forme plus faible de la conjecture de Hall est la suivante:

Conjecture 10. *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tous les entiers $x > 1$ et $y > 0$ on ait:*

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

On va montrer que cette forme peut être une conséquence de la conjecture *abc*, via la conjecture de Szpiro généralisée.

Proposition 13. *La conjecture abc implique la conjecture 10.*

Preuve. Supposons d'abord que $(x, y) = 1$. Appliquons la conjecture 3 à la relation $x^3 - y^2 = k$. On obtient:

$$x \leq c_1(\varepsilon) \left(r(k)\right)^{2+\varepsilon} \leq c_1(\varepsilon) \left(|k|\right)^{2+\varepsilon}.$$

Alors:

$$|k| \geq c_2(\varepsilon) x^{1/(2+\varepsilon)} = c_3(\varepsilon') x^{1/2-\varepsilon'},$$

en prenant $\varepsilon' = \dfrac{\varepsilon}{2(2+\varepsilon)}$. Par le même raisonnement, on obtient:

$$|k| \geq c_4(\varepsilon') y^{1/3-\varepsilon'},$$

puis l'inégalité de la conjecture 10 lorsque $(x, y) = 1$. Cette inégalité reste valable si on la multiplie par un entier positif quelconque, ce qui donne le cas général. ■

7. L'équation de Mordell. Soit k un entier non nul. L'équation:

$$x^3 - y^2 = k,$$

appelée équation de Mordell n'admet qu'un nombre fini de solutions entières. En 1968, A. Baker a montré que ces solutions vérifient:

$$\log \max(|x|, |y|) < 10^{10} |k|^{10^4}.$$

Cette borne a été ensuite améliorée en 1973 par H. Stark (voir [Sta]), qui a énoncé le théorème suivant:

Théorème 8. (Stark). *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout entier non nul k, toute solution entière de l'équation $x^3 - y^2 = k$ vérifie:*

$$\log \max(|x|, |y|) \leq c(\varepsilon) |k|^{1+\varepsilon}.$$

En 1982, V. G. Sprindzuk, a démontré quand à lui qu'il existe une constante absolue $c > 0$ telle que les solutions de l'équation de Mordell vérifient:

$$\log \max(|x|, |y|) \leq c|k|(\log |k| + 1)^6.$$

Les bornes données par Baker, Stark et Sprindzuk sont cependant très grandes par rapport à ce que peut donner la conjecture *abc*.

Proposition 14. *La conjecture abc implique que pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tout entier non nul k, toute solution entière de l'équation $x^3 - y^2 = k$ vérifie:*

$$\max(|x|^3, y^2) \leq c(\varepsilon)|k|^{6+\varepsilon}.$$

Preuve. La conjecture *abc* implique, via la conjecture 10, que:

$$|x| \leq c_1(\varepsilon)\left(|k|\right)^{2+\varepsilon} \qquad \text{et} \qquad |y| \leq c_2(\varepsilon)\left(|k|\right)^{3+\varepsilon},$$

d'où la conclusion de la proposition. ■

Remarque. La borne qui figure dans cette proposition n'est pas très grande si on la compare aux bornes de Baker et de Stark. On peut illustrer ce fait en considérant le meilleur exemple pour la conjecture de Hall, tiré de la table 3:

$$28187351^3 - 149651610621^2 = -1090.$$

Soit $\varepsilon > 0$ donné. L'inégalité du théoréme de Stark donne:

$$149651610621 \leq \exp\left(1090^{1+\varepsilon} c(\varepsilon)\right),$$

avec $\exp(1090) \simeq 2,4 \times 10^{473}$. La conjecture *abc*, via la conjecture 10 donne:

$$149651610621 \leq 1090^{3+\varepsilon} c(\varepsilon),$$

avec seulement $1090^3 \simeq 1.3 \times 10^9$. ■

8. La conjecture de Pillai. Cette conjecture date de 1945. Elle concerne une classe d'équations diophantiennes.

Conjecture 11. (Pillai). *Soient $A > 0$, $B > 0$ et k des entiers, 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 $mn > 4$.

Lorsque $A = 1, B = 1$ et $k = 1$, cette conjecture s'appelle la conjecture de Catalan, qui, conjecture en plus que la seule solution est $(x, y, m, n) = (3, 2, 2, 3)$. R. Tijdeman a démontré en 1976 que la conjecture de Pillai est vraie dans le cas $A = B = k = 1$ (voir [Sho-Tij]). La conjecture abc répond positivement à la conjecture de Pillai.

Proposition 15. *La conjecture abc implique la conjecture de Pillai.*

Preuve. Tous les entiers qui figurent dans cette preuve sont positifs. Soit $d = (Ax^m, By^n, k)$. Appliquons la conjecture abc au triplet $(Ax^m/d, By^n/d, k/d)$. On obtient:

$$Ax^m/d, By^n/d \leq c_1(\varepsilon)\left(r\left(ABkx^my^n/d^3\right)\right)^{1+\varepsilon},$$

ce qui donne:

$$Ax^m, By^n \leq c_1(\varepsilon)\left(dr\left(ABkx^my^n/d^3\right)\right)^{1+\varepsilon} \leq c_2(\varepsilon, A, B, k)\,(xy)^{1+\varepsilon}, \tag{5}$$

puis

$$x^m, y^n \leq c_3(\varepsilon, A, B, k)\,(xy)^{1+\varepsilon}.$$

Supposons par exemple que $x^m \leq y^n$, alors (5) devient:

$$y^n \leq c_3(\varepsilon, A, B, k)y^{(1+\varepsilon)(1+n/m)},$$

puis:

$$(y^n)^{1-\left(m^{-1}+n^{-1}\right)(1+\varepsilon)} \leq c_3(\varepsilon, A, B, k). \tag{6}$$

Puisque $m \geq 2$, $n \geq 2$ et $mn \geq 6$, alors $m^{-1} + n^{-1} \leq 5/6$ et donc pour ε assez petit, $\left(m^{-1} + n^{-1}\right)(1 + \varepsilon) < 1$. L'inégalité (6) implique alors que y et n sont bornés et donc que x et m le sont aussi. ■

9. Un cas particulier de l'équation de Pell. La conjecture de Pillai exclut le cas $(m, n) = (2, 2)$. Soient $A > 0$, B et k des entiers premiers entre eux. Considérons l'équation:

$$Ax^2 - By^2 = k,$$

en entiers $x \neq 0$, $y \neq 0$ tels que $r(y)$ est borné (c'est le cas si $r(y)|B$).

Proposition 16. *La conjecture abc implique que l'équation de Pell ci-dessus n'admet qu'un nombre fini de solutions telles que $r(y)$ soit borné .*

Preuve. Soit $d = (Ax^2, By^2)$. Appliquons la conjecture *abc* au triplet $(Ax^2/d, By^2/d, k/d)$. On obtient:

$$Ax^2/d \leq c_1(\varepsilon)\left(r(ABkx^2y^2/d^3)\right)^{1+\varepsilon},$$

puis

$$Ax^2 \leq c_1(\varepsilon)\left(d(k/d)r(ABx^2y^2/d^2)\right)^{1+\varepsilon} \leq c_1(\varepsilon)\left(kABr(xy)\right)^{1+\varepsilon}.$$

Alors:

$$x^2 \leq c_2(\varepsilon, A, B, k)\left(|x|\right)^{1+\varepsilon}(r(y)^{1+\varepsilon},$$

et donc

$$|x|^{1-\varepsilon} \leq c_2(\varepsilon, A, B, k)(r(y))^{1+\varepsilon}.$$

Ceci montre donc que $|x|$ est borné, puisque $(r(y)$ l'est. ■

Remarque. C. Störmer [Stö1] a démontré en 1897 que dans le cas $A = 1$, $B > 0$, $k = -1$ et $r(y)|B$, l'équation de Pell ci-dessus admet au plus une solution. ■

10. L' équation de Fermat généralisée. La conjecture *abc* et les conjectures de Szpiro, via la conjecture 4, s'appliquent particulièrement aux équations diophantiennes à trois termes. En voici un exemple.

Théorème 9. *Si la conjecture abc est vraie et si A, B, C sont des entiers strictement positifs, alors l'équation:*

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

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

Preuve. Supposons que $(x, y, z) = 1$. Si $z = 1$, on a la conclusion de la conjecture de Pillai. Supposons donc que $z \geq 2$. 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:

$$Cz^n/d \leq c_1(\varepsilon)\left(r(ABCx^ly^mz^n/d^3)\right)^{1+\varepsilon},$$

d'où l'on tire:

$$z^n \leq c_1(\varepsilon)/C\left(dr(ABCx^ly^mz^n/d^3)\right)^{1+\varepsilon} \leq c_2(\varepsilon, A, B, C)\left(xyz\right)^{1+\varepsilon}.$$

Puisque $Ax^l < Cz^n$ et $By^m \leq Cz^n$, alors $x < c_3(A, C)z^{n/l}$ et $y < c_4(B, C)z^{n/m}$. Ainsi

$$z^n \leq c_5(\varepsilon, A, B, C)\left(z^n\right)^{(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})},$$

ce qui donne :

$$(z^n)^{1-(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})} \le c_4(\varepsilon, A, B, C).$$

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

Remarque. R. Tijdeman [Tij] affirme ne connaître que les deux solutions:

$$13^2 + 7^3 = 2^9,$$
$$17^3 + 2^7 = 71^2,$$

pour l'équation:

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

en entiers positifs $x, y, z, l > 0, m > 0, n > 0$ avec $l^{-1}+m^{-1}+n^{-1} < 1$. En voici deux autres:

$$2^5 + 7^2 = 3^4,$$
$$3^5 + 11^4 = 2^2.61^2.$$

Ces exemples ont été déterminé comme sous-produits de la recherche de bons exemples pour les conjectures de Szpiro et la conjecture *abc*. ■

11. La conjecture de Shorey-Tijdeman. Dans la page 202 de leur livre "Exponential Diophantine Equations", Shorey et Tijdeman [Sho-Tij] proposent la conjecture suivante:

Conjecture 12. *L'équation diophantienne*

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

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* $mn > 4$.

Si l'une des variables v, w, x ou y est composée de nombres premiers fixés, cette conjecture est vraie ([Sho-Tij], p. 202). La conjecture *abc* peut répondre affirmativement à la conjecture de Shorey et Tijdeman avec une condition supplémentaire sur les exposants m et n.

Proposition 17. *La conjecture abc implique la conjecture* 12.

Preuve. Supposons que $(v, x) = (w, y) = 1$. Si $v = 1$, alors $w = 1$ et la proposition découle de l'équation de Catalan. Supposons donc que $v > 1$ et $w > 1$. De l'égalité:

(7) $$w^n x^m - v^m y^n = v^m w^n,$$

on tire d'une part $w^n x^m = v^m(w^n + y^n)$ et donc $v^m | w^n$, et d'autre part $v^m y^n = w^n(x^m - v^m)$ et donc $w^n | v^m$. Ainsi on a $v^m = w^n$ et donc il existe un entier $z > 1$ tel que $v^m = w^n = z^{<m,n>}$ où $< m, n >$ désigne le plus petit multiple commun de m et de n. En simplifiant l'égalité (7) par $z^{<m,n>}$, on obtient la relation:

$$x^m - y^n = z^{<m,n>},$$

qui, d'après le théorème 9 n'admet qu'un nombre fini de solutions qui vérifient l'inégalité $m^{-1} + n^{-1} + (< m, n >)^{-1} < 1$. Cette dernière condition est réalisée si $m \geq 2$, $n \geq 2$ et $mn > 4$ sauf pour $(m, n) = (2, 3), (3, 2), (3, 3), (2, 4), (4, 2)$. Considérons ces cas particuliers:
- Si $(m, n) = (2, 3)$, on peut transformer l'équation $x^2 - y^3 = z^6$ en la courbe elliptique $Y^2 = X^3 + 1$ qui n'admet qu'un nombre fini de points rationnels.
- Si $(m, n) = (3, 2)$, on aboutit à la courbe elliptique $Y^2 = X^3 - 1$ qui n'admet aussi qu'un nombre fini de points rationnels.
- Si $(m, n) = (3, 3)$, l'équation $x^3 - y^3 = z^3$ n'a pas de solution non triviale (Théorème d'Euler).
- Si $(m, n) = (2, 4)$, l'équation $x^2 - y^4 = z^4$ n'a pas de solution non triviale ([Mord], p. 16).
- Si $(m, n) = (4, 2)$, l'équation $x^4 - y^2 = z^4$ n'a pas de solution non triviale ([Mord], p. 17). ■

12. Une équation en S-entiers. Soient $p_1, \cdots p_s$ des nombres premiers distincts. On considère l'équation diophantienne

$$p_1^{l_1} p_2^{l_2} \dots p_s^{l_s} \pm p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} = y^n,$$

en entiers positifs y, n, l_1, $\cdots$,l_s, m_1, $\cdots$, m_s avec pour tout i, $l_i m_i = 0$.

Proposition 18. *La conjecture abc entraîne que l'équation ci-dessus n'admet qu'un nombre fini de solutions avec $y > 1$ et $n \geq 2$.*

Preuve. Appliquons la conjecture *abc* à la relation

$$p_1^{l_1} p_2^{l_2} \dots p_s^{l_s} \pm p_1^{m_1} p_2^{m_2} \dots p_s^{m_s} = y^n.$$

On obtient:

$$y^n \leq c_1(\varepsilon)(p_1 \dots p_s)^{1+\varepsilon} y^{1+\varepsilon},$$

et donc:

$$y^{n-1-\varepsilon} \leq c_2(\varepsilon, p_1, \cdots, p_s).$$

Ceci montre que si $y > 1$, n et y sont bornés et que les l_i et m_i le sont aussi. ■

13. Quelques conjectures sur les nombres puissants. Commençons par donner la définition d'un nombre puissant:

Définition 3. *Un entier n est un nombre puissant si:*

$$(r(n))^2 \,|n.$$

Il est évident que tout nombre puissant n s'écrit de façon unique sous la forme $n = a^2b^3$, où b est sans facteurs carrés. D'autre part, le radical $r(n)$ d'un nombre puissant vérifie $r(n) \leq n^{1/2}$. Cette propriété du radical sera utilisée abondamment dans ce paragraphe.
Dans [Rib2], P. Ribenboim étudie le lien entre les nombres puissants et le dernier théorème de Fermat. Il étudie aussi quelques conjectures relatives à ces nombres. Ces conjectures étant nombreuses, nous nous contentons de trois d'entre elles, et nous montrons qu'elles sont parfois des conséquences de la conjecture *abc*. Certaines de ces conjectures se trouvent aussi dans [Guy] (B 16).

Conjecture 13. (Erdös-Mollin-Walsh). *Il n'y a aucun triplet de nombres puissants consécutifs.*

Cette conjecture implique en particulier qu'il existe une infinité de nombres premiers p tels que

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

ce qui fait apparaître un lien avec le premier cas du dernier théorème de Fermat (voir conjecture 7 ou [Rib2]).
La conjecture *abc* ne permet pas de répondre catégoriquement à la conjecture 13, mais permet d'avoir ceci:

Proposition 19. *La conjecture abc implique qu'il n'y a qu'un nombre fini de triplets de nombres puissants consécutifs.*

Preuve. Si $1 < a < b < c$ sont trois nombres consécutifs, alors ils vérifient la relation:

$$b^2 = ac + 1.$$

Supposons que les nombres a, b , c sont puissants. En appliquant la conjecture *abc* à cette relation, on obtient:

$$b^2 \leq c(\varepsilon)(r(abc))^{1+\varepsilon} \leq c(\varepsilon)(abc)^{(1+\varepsilon)/2} \leq c(\varepsilon)b^{3(1+\varepsilon)/2},$$

d'où:

$$b^{(1-3\varepsilon)/2} \leq c(\varepsilon).$$

Ainsi, si ε est assez petit, b, puis a et c sont bornés. ■

La conjecture suivante concerne des nombres généralisant les nombres de Fermat et de Mersenne:

Conjecture 14. *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 $\lim\limits_{k\to\infty} |2^k - n_k| = +\infty$.*

Nous avons alors la conséquence suivante de la conjecture *abc*.

Proposition 20. *La conjecture abc implique la conjecture* 14.

Preuve. Soit $k \geq 2$. Il est évident que le nombre puissant n_k le plus proche et distinct de 2^k est de la forme $n_k = 2^s n'_k$ avec $s = 0$ ou $1 < s < k$ et où n'_k est un nombre puissant impair. On considère alors la relation:

$$2^{k-s} - n_k/2^s = z.$$

Appliquons la conjecture *abc* à cette relation. On obtient:

$$n_k/2^s \leq c(\varepsilon)\left(r(n_k z/2^s)\right)^{1+\varepsilon}.$$

Alors:

$$n_k \leq c(\varepsilon)\left(2^s z r(n_k/2^s)\right)^{1+\varepsilon} \leq c(\varepsilon)|2^k - n_k|^{1+\varepsilon} n_k^{(1+\varepsilon)/2},$$

et donc:

$$n_k^{(1-\varepsilon)/2} \leq c(\varepsilon)|2^k - n_k|^{1+\varepsilon}.$$

Remarquons d'abord que $\lim\limits_{k\to\infty} n_k = \infty$. En fixant ε assez petit, on obtient la conclusion de la conjecture 14 en faisant tendre k vers l'infini. ■

La conjecture suivante concerne directement les nombres de Fermat et de Mersenne.

Conjecture 15. *Il existe une infinité de nombres de Fermat et de Mersenne qui ne sont pas des nombres puissants.*

Nous avons de même la conséquence suivante.

Proposition 21. *La conjecture abc implique la conjecture* 15.

Preuve. Il suffit de montrer que la conjecture *abc* implique qu' il n'existe qu'un nombre fini de nombres de Fermat et de Mersenne qui sont des nombres puissants. Plus généralement, considérons l'équation diophantienne:

$$2^k \pm 1 = z,$$

en entiers $k \geq 1$ et en nombre puissant z. D'après la proposition 20, cette équation n'admet qu'un nombre fini de solutions. Les nombres de Fermat et de Mersenne étant en nombre infini, ceci termine la preuve de la proposition. ■

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 B 16 de [Guy]).

Conjecture 13. (Erdös) *L'équation*

$$x + y = z,$$

n'admet qu'un nombre fini de solutions en entiers positifs 4*-puissants* x*,* y *et* z *premiers entre eux.*

Il est alors facile de voir que cette conjecture est une conséquence de la conjecture *abc*.

Proposition 22. *La conjecture abc implique la conjecture* 16*.*

Preuve. Appliquons la conjecture *abc* au triplet (x, y, z) de nombres 4-puissants vérifiant $(x, y, z) = 1$ et $x + y = z$. On obtient:

$$z \leq c(\varepsilon) \left(r(xyz)\right)^{1+\varepsilon} \leq c(\varepsilon)(xyz)^{(1+\varepsilon)/4} \leq c(\varepsilon) z^{3(1+\varepsilon)/4}.$$

Finalement:

$$z^{(1-3\varepsilon)/4} \leq c(\varepsilon),$$

et donc z est borné, d'où la conclusion de la conjecture 16. ■

14. La conjecture de Calderbank. En 1982, R. Calderbank avait proposé la conjecture suivante.

Conjecture 17. (Calderbank). *Pour tout entier* $q \neq 3$ *de la forme* $q = p^k$ *où* p *est un nombre premier et où* $k \geq 1$*, l'équation diophantienne*

$$y^2 = 4q^n + 4q + 1,$$

en entiers $y \geq 1$ et $n \geq 2$ n'admet que la solution $(y, n) = (2q+1, 2)$.

Plusieurs travaux ont montré que cette conjecture est vraie pour des valeurs particulières de q. Par exemple, N. Tzanakis et J. Wolfskill [Tza-Wol] l' ont montré pour $q = 3^k$ avec $k \geq 2$. Ils ont montré aussi que l'équation de Calderbank n'a pas de solutions avec $n \geq 3$ si q est un carré parfait et qu'elle admet au plus une solution avec $n \geq 3$ si $q = p^k > 200$. Mais dans le cas général, la conjecture de Calderbank n'est pas démontrée.
La conjecture *abc* peut aussi être appliquée à la conjecture de Calderbank, mais ne peut pas la confirmer totalement. Elle implique tout simplement que l'équation de Calderbank n'a qu'un nombre fini de solutions avec $n \geq 3$, sans se soucier de la nature de q.

Proposition 23. *La conjecture abc implique que l'équation*

$$y^2 = 4q^n + 4q + 1,$$

en entiers $y \geq 1$, $q \geq 2$ et $n \geq 3$ n'admet qu'un nombre fini de solutions.

Preuve. Appliquons la conjecture *abc* au triplet $(y^2, 4q^n, 4q+1)$. On obtient:

$$y^2 \leq c_1(\varepsilon)(q(4q+1)y)^{1+\varepsilon}.$$

L'inégalité $q^n < y^2$ donne $q < y^{2/n}$ et donc $4q + 1 < 5y^{2/n}$. Alors

$$y^{2-(1+4n^{-1})(1+\varepsilon)} \leq c_2(\varepsilon).$$

Pour ε assez petit et pour $n \geq 5$, ceci montre que y est borné. La relation $y^2 = 4q^n + 4q + 1$ montre alors que n et q sont bornés. Il reste à considérer les cas $n = 3$ et $n = 4$. Le théorème de Siegel (voir [Sil-Tat], p. 146) assure la finitude du nombre de solutions en entiers de l'équation dans ces cas là. ■

Remarque. Soient a, b, c, d des entiers non nuls. Suivant le même principe, on peut montrer que la conjecture *abc* implique que l'équation diophantienne

$$ay^2 = bq^n + cq + d,$$

n'admet qu'un nombre fini de solutions en entiers $y \geq 1$, $q \geq 2$ et $n \geq 3$.

15. Le problème de Brocard. Récemment (mai 1993), M. Overholt ([Ove]) a montré que les conjectures de Szpiro impliquent que l'équation:

$$x! + 1 = y^2,$$

n'a qu'un nombre fini de solutions $x > 0$ et $y > 0$. Déterminer les solutions de cette équation a été soulevé par H. Brocard en 1876.
On peut généraliser ce résultat en appliquant cette fois la conjecture abc pour montrer que l'équation

$$(x!)^n + 1 = y^m, \tag{8}$$

en entiers $x > 0$, $y > 0$, $n > 0$ et $m > 1$ n'a qu'un nombre fini de solutions.
On aura besoin des deux inégalités suivantes, déduites respectivement des formules de Stirling et de Chebytshev ([Ni-Zu-Mo], p. 374) et qui sont vérifiées pour tout entier positif x:

$$\begin{cases} (x/e)^x < x!, \\ \prod_{p \leq x} p < 4^x, \ p \text{ premier.} \end{cases} \tag{9}$$

Proposition 24. *La conjecture abc implique que l'équation* (8) *n'a qu'un nombre fini de solutions* $x > 0$, $y > 0$, $n \geq 1$ *et* $m \geq 2$.

Preuve. Appliquons la conjecture abc au triplet $((x!)^n, 1, y^m)$. On obtient:

$$(x!)^n \leq c_1(\varepsilon)\left(r(y(x!))\right)^{1+\varepsilon} \leq c_1(\varepsilon)\left(yr(x!)\right)^{1+\varepsilon}.$$

En utilisant l'inégalité $y^m \leq 2(x!)^n$, on obtient:

$$(x!)^n \leq c_2(\varepsilon)\left((x!)^{n/m}\right)^{1+\varepsilon}\left(\prod_{p\leq x} p\right)^{1+\varepsilon},$$

ce qui donne:

$$\left((x!)^n\right)^{1-\frac{(1+\varepsilon)}{m}} \leq c_2(\varepsilon)\left(\prod_{p\leq x} p\right)^{1+\varepsilon}.$$

En utilisant les inégalités (9), on obtient:

$$\left((x/e)^{nx}\right)^{1-\frac{1+\varepsilon}{m}} \leq c_2(\varepsilon)4^{x(1+\varepsilon)},$$

d'où:

$$\left((x/e)^{n}\right)^{1-\frac{1+\varepsilon}{m}} \leq c_3(\varepsilon)4^{(1+\varepsilon)}.$$

Il en résulte alors pour ε assez petit et pour $m \geq 2$ que x est borné. Si $x = 2$, alors il n'y a qu'un nombre fini de solutions pour l'équation (8) avec $m \geq 2$. Maintenant pour $m \geq 2$ et $x \geq 3$, l'inégalité ci-dessus implique que x et n, puis y et m sont bornés. ■

Remarque. Je ne connais que les solutions suivantes de l'équation (7):

$$\begin{aligned} &4! + 1 = 5^2, \quad 5! + 1 = 11^2, \\ &7! + 1 = 71^2, \quad (2!)^3 + 1 = 3^2. \end{aligned}$$

16. La conjecture d'Erdös-Stewart. Soit $p_1, p_2, \cdots, p_k, \cdots$ la suite croissante des nombre premiers. Dans [Guy] (p. 6), P. Erdös et C.L. Stewart proposent la conjecture suivante:

Conjecture 18. (Erdös-Stewart). *L'équation*

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

en entiers n, $a \geq 0$, $b \geq 0$ et $p_{k-1} \leq n < p_k$ n'admet que les solutions $1!+1 = 2$, $2!+1 = 3$, $3! + 1 = 7$, $4! + 1 = 5^2$ et $5! + 1 = 11^2$.

La conjecture *abc* répond partiellement à cette conjecture.

Proposition 25. *La conjecture abc entraîne qu'il n'y a qu'un nombre fini de solutions pour la conjecture d'Erdös-Stewart.*

Preuve. Appliquons la conjecture *abc* au triplet $(n!, 1, p_k^a p_{k+1}^b)$. On obtient:

$$n! \leq c_1(\varepsilon)\left(r(n! p_k p_{k+1})\right)^{1+\varepsilon} \leq c_1(\varepsilon)\left(\prod_{p \leq p_{k+1}} p\right)^{1+\varepsilon}. \tag{10}$$

En utilisant les inégalités (9) et le postulat de Bertrand qui permet d'avoir $p_{k+1} < 2p_k < 4p_{k-1} \leq 4n$, (10) devient:

$$(n/e)^n \leq c_1(\varepsilon) 4^{(1+\varepsilon)p_{k+1}} \leq c_1(\varepsilon) 4^{4(1+\varepsilon)n}.$$

Alors $n/e \leq c_2(\varepsilon) 4^{4(1+\varepsilon)}$, ce qui implique que n est borné. ■

On peut généraliser la conjecture d'Erdös-Stewart par la conjecture suivante, et il est facile de montrer que c'est une conséquence de la conjecture *abc*, sauf pour un nombre fini de cas.

Conjecture 17. *Soit u un entier donné. L'équation*

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

n'admet qu'un nombre fini de solutions en entiers $n \geq 2$, $a, b \geq 0$ et en nombres premiers p_k et p_{k+1} vérifiant $p_{k-u} \leq n < p_k$.

17. Un problème de Ghandi. J. M. Ghandi (voir [Guy] D 2) se demande si l'équation

$$x^n + y^n = n!z^n, \tag{11}$$

peut avoir des solutions en entiers x, y, z et $n \geq 3$. On remarque d'abord que si $n = 2$, il existe une infinité de solutions. En effet si on définit deux suites (x_k) et (y_k) d'entiers par la relation:

$$x_k + y_k\sqrt{2} = (1 + \sqrt{2})^k,$$

alors pour tout $k \geq 0$, $x_k^2 - 2y_k^2 = (-1)^k$ et en particulier si k est inpair, alors $1 + x_k^2 = 2y_k^2$ est une réponse pour la question de Ghandi avec $n = 2$. Si maintenant $n = 3$, alors il existe aussi une infinité de solutions définies par les relations de récurrences:

$$x_0 = 37, y_0 = 17, z_0 = 21,$$

et pour tout $k \geq 0$,

$$\begin{aligned} x_{k+1} &= x_k(x_k^3 + 2y_k^3), \\ y_{k+1} &= -y^k(2x_k^3 + y_k^3), \\ z_{k+1} &= z_k(x_k^3 - y_k^3). \end{aligned}$$

Il reste donc à considérer les cas $n \geq 4$. La conjecture *abc* peut répondre partiellement au problème de Ghandi.

Proposition 26. *La conjecture abc entraîne que l'équation* (11) *n'a qu'un nombre fini de solutions $x > 0$, $y > 0$, $z > 0$ et $n \geq 4$.*

Preuve. Supposons que les entiers positifs x, y, z et $n \geq 3$ forment une solution de l'équation (11). On peut supposer que $(x, z) = 1$. D'autre part, le pgcd d de x^n et à $n!$ est de la forme d^n et donc on doit avoir $d^n | n!$ ce qui est impossible si $d > 1$. Appliquons alors la conjecture *abc* à l'égalité $x^n + y^n = n!z^n$. Nous obtenons:

$$n!z^n \leq c_1(\varepsilon)(xyz)^{1+\varepsilon} r(n!)^{1+\varepsilon},$$

En utilisant les majorations $x, y, z \leq (n!z^n)^{1/n}$, on obtient:

$$n!z^n \leq c_1(\varepsilon)(n!z^n)^{3(1+\varepsilon)/n} \left(r(n!)\right)^{1+\varepsilon},$$

puis, en utilisant les formules (9):

$$(nz/e)^{n(1-3(1+\varepsilon)/n)} \leq (n!z^n)^{1-3(1+\varepsilon)/n} \leq c_1(\varepsilon)4^{n(1+\varepsilon)},$$

ce qui donne:

$$(nz/e)^{1-3(1+\varepsilon)/n} \leq c_2(\varepsilon)4^{1+\varepsilon}.$$

Ceci implique donc n et z sont bornés et donc l'équation (11) ne peut avoir qu'un nombre fini de solutions avec $n \geq 4$. ■

18. Le problème de Simmons. Dans [Guy] (D 25), Simmons se demande si les seules solutions de l'équation diophantienne

$$n! = m(m^2 - 1)$$

en entiers positifs sont $(n, m) = (3, 2), (4, 3), (5, 5)$ et $(6, 9)$. On peut généraliser ce problème en considérant l'équation:

$$n! = m(m^k \pm 1),$$

en entiers positifs $n > 1$, $m > 1$, $k \geq 2$.

Proposition 27. *La conjecture abc entraîne que l'équation ci-dessus n'admet qu'un nombre fini de solutions.*

Preuve. Ecrivons

$$m^k \pm 1 = n!/m,$$

et appliquons la conjecture *abc*. On obtient:

$$n!/m \leq c_1(\varepsilon)\left(r(n!)\right)^{1+\varepsilon}.$$

En utilisant l'inégalité:

$$m^k \leq 2n!/m,$$

et les inégalités (9), on obtient:

$$(n/e)^{nk/(k+1)} \leq (n!)^{k/(k+1)} \leq c_1(\varepsilon)2^{1/(k+1)}4^{n(1+\varepsilon)},$$

puis

$$(n/e)^{k/(k+1)} \leq c_2(\varepsilon),$$

ce qui implique que n est borné. Alors m et k sont bornés aussi. ■

19. Un problème d'Edgar et de Shorey-Tijdeman. D'après [Guy] (D 10), H. Edgar se demande si l'équation

$$1 + x + x^2 + \ldots + x^{n-1} = \frac{x^n - 1}{x - 1} = z^m,$$

en entiers premiers x, z, $n \geq 5$ et $m \geq 2$, admet d'autres solutions que $1 + 3 + 3^2 + 3^3 + 3^4 = 11^2$ (voir aussi [Sho-Tij] p. $202 - 203$). Nous allons considérer ce problème plus généralement. Soit a un entier positif. On considère l'équation:

$$x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1} = \frac{x^n - y^n}{x - y} = az^m, \tag{12}$$

en entiers $x > y > 0$, $z > 0$, $n > 3$, $m > 1$.

Proposition 28. *La conjecture abc entraîne que l'équation* (12) *n'a qu'un nombre fini de solutions* $x > y > 0$, $z > 0$, $n > 3$, $m > 1$ *avec* $(x, y) = 1$, $3n^{-1} + m^{-1} < 1$.

Preuve. Supposons que $0 < y < x$ et $(x, y) = 1$. Appliquons la conjecture *abc* à la relation suivante, déduite de l'équation (12):

$$y^n + az^m(x - y) = x^n,$$

et en utilisant les inégalités $x - y < x$ et $z \leq x^{m/n}$, on obtient:

$$x^n \leq c_1(\varepsilon)\left(ayz(x-y)x\right)^{1+\varepsilon} \leq c_2(\varepsilon, a)x^{(3+n/m)(1+\varepsilon)}.$$

D'où l'on tire:

$$(x^n)^{1-(3n^{-1}+m^{-1})(1+\varepsilon)} \leq c_2(\varepsilon, a).$$

Si ε est assez petit et si $3n^{-1} + m^{-1} < 1$, alors x, n, puis y, z et m sont bornés. ∎

Remarque. Si f est une forme binaire à coefficients dans $\mathbb{Z}$ avec $f(1, 0) \neq 0$ et au moins deux facteurs linéaires distincts sur $\mathbb{Q}$, alors l'équation $f(x, y) = z^m$ en entiers x, y, z et m vérifiant $(x, y) = 1$ et y composé de nombres premiers fixés implique que m est borné (voir [Sho-Tij], p. 170). ∎

20. Le problème de Goormaghtigh. Ce problème consiste à determiner les entiers qui s'écrivent de deux façons différentes sous la forme (voir [Guy], B 25):

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1.} \tag{13}$$

Cela équivaut donc à résoudre cette équation en entiers $m > n > 2$ et $y > x > 1$. Des solutions connues sont $(x, y, m, n) = (2, 5, 5, 3), (2, 90, 13, 3)$. R. Balasubramanian et T.N Shorey (cités dans [Sho-Tij], p.203) ont démontré que si x et y sont composés de nombres premiers fixés, alors l'équation (13) n'admet qu'un nombre fini de solutions en entiers vérifiant $m > n > 2$ et $y > x > 1$. La conjecture abc permet d'avoir le même résultat avec $(x, y) = 1$, et plus généralement:

Proposition 29. *La conjecture abc implique que l'équation* (13) *n'admet qu'un nombre fini de solutions en entiers vérifiant* $m > n > 3$ *et* $y > x > 1$.

Preuve. L'équation (13) donne

$$x^m(y-1) = y^n(x-1) + (y-x).$$

Soit $d = (x^m(y-1), y^n(x-1))$. Appliquons maintenant la conjecture abc au triplet $(x^m(y-1)/d, y^n(x-1)/d, (y-x)/d)$. On obtient:

$$x^m(y-1)/d <\leq c_1(\varepsilon)\left(r\left(x^m y^n(y-1)(x-1)(y-x)/d^3\right)\right)^{1+\varepsilon},$$

ce qui donne:

$$\begin{aligned} yx^m &\leq c_2(\varepsilon)\left((y-x)r(x^m y^n(x-1)(y-1)/d^2\right)^{1+\varepsilon} \\ &\leq c_2(\varepsilon)\left((y-x)r(x^m y^n(x-1)(y-1)\right)^{1+\varepsilon} \\ &\leq c_2(\varepsilon)\left((y-x)xy(x-1)(y-1)\right)^{1+\varepsilon}. \end{aligned}$$

La relation (13) montrer que y et $x^{(m-1)/(n-1)}$ sont de même ordre de grandeur. Alors:

$$x^{m+(m-1)/(n-1)} \leq c_3(\varepsilon)\left(x^{2+3(m-1)/(n-1)}\right)^{1+\varepsilon},$$

et donc

$$x^{(mn-1-(2n+3m-5)(1+\varepsilon))/(n-1)} \leq c_2(\varepsilon).$$

Supposons que ε est assez petit. Si $m > n > 3$, alors $mn - 1 > 2n + 3m - 5$ et donc l'inégalité ci-dessus montre que x, m, n, et y sont bornés. ∎

21. Les progressions arithmétiques. Soient m, d et k des entiers positifs tels que $(m, d) = 1$ et $k \geq 3$. Considérons le produit:

$$\Pi = m(m+d)\cdots(m+(k-1)d),$$

des k termes de la progression arithmétique $m, m+d, \cdots, m+(k-1)d$. En 1975, P. Erdös et J.L. Selfridge ont montré que lorsque $d = 1$, Π ne peut pas être de la forme y^n avec

$n, y \geq 2$. En 1985, R. Marzsalek a montré que k peut être borné en fonction de d lorsque $n \geq 2$(voir [Tij]).
Nous verrons dans cette partie comment appliquer la conjecture *abc* à ce problème. Montrons d'abord le lemme suivant:

Lemme 3. *Soient i et j deux entiers vérifiant $0 < i < j \leq k-1$, alors $(m+id, m+jd) < k$.*

Preuve. Soient i et j deux entiers vérifiant $0 \leq i < j \leq k-1$. Soit $g = (m+id, m+jd)$. Alors $g|(j-i)d$. Si p est un facteur premier de g et $p|d$, alors $p|m$, d'où $p = 1$. Ainsi $p|j-i < k$ et donc $g < k$. Ceci montre en particulier que les termes $m+id$ et $m+jd$ n'ont aucun facteur premier commun p tel que $p \geq k$. ■

Remarque. D'après ce qui précède, pour tout i, $0 \leq i \leq k-2$, $(m+id, m+(i+1)d) = 1$ et pour tout i, $0 \leq i \leq k-3$, $(m+id, m+(i+2)d) \leq 2$.

Proposition 30. *La conjecture abc implique que pour tout $d \geq 1$, l'équation $m(m+d)\dots(m+(k-1)d) = y^n$ n'admet qu'un nombre fini de solutions en entiers $m > 0$, $k \geq 3$, $y > 0$, $n \geq 2$.*

Preuve. Nous allons le montrer avec $k = 3$. En utilisant le lemme 3, on a pour tout $i, 0 \leq i \leq 2$:

$$m + id = a_i y_i^n,$$

en désignant par a_i la partie contenant les facteurs premiers inférieurs à 3 et par y_i la partie contenant les facteurs supérieurs ou égaux à 3, avec la possibilité $y_i = 1$. Rappelons que $(m+d, m(m+2d)) = 1$, ce qui montre que $a_1 = 1$ et $y_1 \geq 2$. La relation $(m+d)^2 = d^2 + m(m+2d)$ donne alors:

$$a_1 y_1^{2n} = d^2 + a_0 a_2 y_0^n y_2^n.$$

En appliquant la conjecture *abc*, on obtient:

$$y_1^{2n} \leq c(\varepsilon, d) \left(r(y_0 y_1 y_2) \right)^{1+\varepsilon} \leq c_1(\varepsilon, d) y_1^{3(1+\varepsilon)},$$

puis

$$y_1^{2n-3(1+\varepsilon)} \leq c_1(\varepsilon, d).$$

Cette inégalité montre que n est borné et que si $n \geq 2$, y_1, puis y_2 et y_3 le sont aussi. ■

22. La conjecture de Richard. Un résultat curieux est le fait que la conjecture *abc* permet de répondre affirmativement à la conjecture suivante , citée dans [Ric]:

Conjecture 20. (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.

Nous allons reprendre la démonstration donnée dans [Ric]. On aura besoin du lemme suivant:

Lemme 4. *Si la conjecture abc est vraie, alors pour tout $\varepsilon>0$, il existe une constante positive $c(\varepsilon)$ telle que pour tous les entiers $x>1$ et $n>0$ on ait:*

$$r(x^n-1)\geq c(\varepsilon)x^{n(1-\varepsilon)-1}.$$

Preuve. Appliquons la proposition 5 à la relation $(x^n-1)+1=x^n$. On obtient:

$$c(\varepsilon)x^{n(1-\varepsilon)}\leq r(x(x^n-1))\leq xr(x^n-1),$$

ce qui donne le résultat du lemme. ■

Théorème 10. (Schinzel). *Si la conjecture abc est vraie, alors les conditions*

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

pour tout entier n, impliquent que x=y.

Preuve. Supposons que pour tout entier n:

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

Choisissons ε tel que $x^{1-\varepsilon}=(x(x-1))^{1/2}$ et n tel que $(x-1)^{2^{n-1}}<c(\varepsilon)x^{2^{n-1}-1}$. Supposons que $x>y$, alors on a:

$$y^{2^n}-1<(x-1)^{2^n}<c(\varepsilon)x^{2^{n-1}-1}(x-1)^{2^{n-1}}=c(\varepsilon)x^{2^n(1-\varepsilon)-1}\leq r\left(x^{2^n}-1\right)$$

d'où l'on tire:

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

ce qui n'est pas possible avec $y>1$. ■

23. Le problème de Croft. Le problème de savoir dans quelle mesure $|n! - 2^m|$ peut être petit par rapport à 2^m s'appelle le problème de Croft (voir [Guy], F 23). La conjecture *abc* et des résultats expérimentaux (voir Table 4) nous ont motivé pour proposer la conjecture suivante.

Conjecture 21.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:*

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

La conjecture *abc* implique une forme plus faible.

Proposition 31. *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:*

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

Preuve. Posons $n! = 2^s n'$ où n' est impair. Il est clair que $s < n$. On va distinguer deux cas suivant les valeurs de s par rapport à celles de m.
- Si $s \ge m$, alors en appliquant la conjecture *abc* à la relation

$$n!/2^m - 1 = k,$$

il vient:

$$n!/2^n \le n!/2^m \le c_1(\varepsilon)\,(r(n!k))^{1+\varepsilon} \le c_1(\varepsilon)\,(r(n!2^m k))^{1+\varepsilon}\,,$$

et donc en utilisant les inégalités (9), on a:

$$(n/2e)^n \le c_1(\varepsilon)4^{(1+\varepsilon)n}\,(r(2^m k))^{1+\varepsilon}\,.$$

On obtient finalement:

$$n \le c_2(\varepsilon)\,(r(n! - 2^m))^{(1+\varepsilon)/n}\,.$$

- Si $s < m$, alors en appliquant la conjecture *abc* à la relation:

$$n!/2^s - 2^{m-s} = k,$$

il vient:

$$n!/2^n \le n!/2^s \le c(\varepsilon)\,(r(n!2^s k))^{1+\varepsilon}\,.$$

Le résultat s'obtient comme ci-dessus. ∎

Pour illustrer la conjecture 21, nous avons résumé dans la table 4 les valeurs de n et de m pour lesquelles, on a $|\tau| < 10^{-5}$ où τ est le rapport

$$\tau = \frac{2^m - n!}{2^m}.$$

Ces valeurs sont liées par la relation $m \log 2 \simeq \log n!$ et testées pour $n \leq 10^6$.

Table 4

n	2	55139	95868	219536	235928	298981	317032	323909
m	1	788943	1448198	3578755	3870478	5007045	5336158	5461937
$10^5 \times \tau$	0	0.183	-7.333	-5.947	-0.514	-4.664	7.389	1.190

n	326197	404208	440912	464848	513545	522223	598811
m	5503831	6945130	7631067	8080791	9001138	9165866	10628335
$10^5 \times \tau$	2.417	8.016	4.803	-9.884	-2.870	-2.502	-4.751

n	610651	652834	684122	703242	706639	809873
m	10855733	11668545	12273980	12644982	12710976	14727261
$10^5 \times \tau$	9.163	-5.299	-2.331	3.622	5.259	-6.750

n	836705	837752	857077
m	15254536	15275136	15655697
$10^5 \times \tau$	6.120	-1.036	9.384

V. Résultats en faveur des conjectures abc et de Szpiro

Les conjectures *abc* et de Szpiro traîtent beaucoup d'équations diophantiennes. Elles impliquent en particulier que le nombre de solutions est borné dans beaucoup de cas. Inversement, plusieurs résultats, complètement établis confirment en partie la véracité des conjectures *abc* et de Szpiro. Il est bien entendu impossible d'énumérer tous ces résultats. On peut cependant en analyser quelques-uns d'essentiels dans ce domaine.

1. Le théorème de Mahler.

Soit S l'ensemble des entiers positifs composés de s nombres premiers $p_1, p_2, \cdots p_s$ fixés avec $s \geq 2$. On sait depuis Mahler (1933) que l'équation:

$$x + y = z, \tag{14}$$

n'a qu'un nombre fini de solutions dans S (voir aussi [Sho-Tij], p. 41). Ce résultat va dans le même sens que la conjecture abc (et donc les conjectures de Szpiro) en ce sens que celle-ci implique pour la relation (14) que:

$$z \leq c(\varepsilon)\left(r(xyz)\right)^{1+\varepsilon} \leq c(\varepsilon)(p_1 \cdots p_s)^{1+\varepsilon},$$

ce qui implique que z, puis x et y sont bornés. ∎

2. Une inégalité en éléments de S. Soit S l'ensemble des entiers positifs composés de s nombres premiers $p_1, p_2, \cdots p_s$ fixés avec $s \geq 2$. Soit α un réel vérifiant $0 < \alpha < 1$. On considère l'inéquation diophantienne:

$$|x - y| \leq \max(x, y)^{\alpha}, \tag{15}$$

en entiers $x \in S$ et $y \in S$ avec $(x, y) = 1$. Les solutions de cette inéquation sont bornées par une constante effectivement calculable qui ne dépend que des nombres premiers p_1, p_2, $\cdots$, p_s. Une démonstration de ce résultat se trouve dans le livre de B.M.M. de Weger [Weg], chapitre 5. La conjecture abc permet d'obtenir la même conclusion, beaucoup plus facilement.

Proposition 32. *La conjecture abc entraîne que pour tout réel α vérifiant $0 < \alpha < 1$, l'inéquation* (15) *n'a qu'un nombre fini de solutions en entiers $x \in S$, $y \in S$, $(x, y) = 1$.*

Preuve. Supposons que $x > y$ et écrivons $x - y = k$. Appliquons alors la conjecture abc. On obtient:

$$x \leq c(\varepsilon)\left(r(xyk)\right)^{1+\varepsilon} \leq c_2(\varepsilon, p_1, \cdots, p_s)|k|^{1+\varepsilon} \leq c_2(\varepsilon, p_1, \cdots, p_s)x^{\alpha(1+\varepsilon)}.$$

Alors:

$$x^{1-\alpha(1+\varepsilon)} \leq c_2(\varepsilon, p_1, \cdots, p_s).$$

En choisissant ε tel que $1 - \alpha(1 + \varepsilon) > 0$, x est alors borné et donc y aussi. ∎

3. Des équations à trois termes. Le théorème 9 précise la finitude pour tout triplet (A, B, C) du nombre de solutions de l'équation

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

en entiers positifs x, y, z, l, m, n avec $l^{-1} + m^{-1} + n^{-1} < 1$ et $(x, y) = 1$. Certains résultats vont dans ce sens.

(i) Sierpinski en 1956 (cité dans [Ter]): L'équation $3^x + 4^y = 5^z$ n'admet que la solution $(x, y, z) = (2, 2, 2)$ en entiers positifs.

(ii) Jesmanowicz en 1956 (cité dans [Ter]): Les équations $5^x + 12^y = 13^z$, $7^x + 24^y = 25^z$, $9^x + 40^y = 41^z$, $11^x + 60^y = 61^z$ n'admettent que les solutions $(x, y, z) = (2, 2, 2)$ en entiers positifs.

(iii) Terai en 1993 [Ter]: Ses résultats sont récents et on y trouve:

Théorème 11. (Terai). *Soient p et q deux nombres premiers vérifiant:*
(a) $q^2 + 1 = 2p$,
(b) $d = 1$ *ou* d *est pair si* $q \equiv 1 \pmod 4$,
où d est l'ordre d'un diviseur premier de (p) dans le groupe des classes d'ideaux de $\mathbb{Q}(\sqrt{-q})$. Alors l'équation

$$x^2 + q^m = p^n,$$

admet la seule solution $(x, m, n) = (p - 1, 2, 2)$.

(v) Scott en 1993 [Sco]: Si $a > 1$, $b > 1$ sont des entiers premiers entre eux, et si p est un nombre premier, alors l'équation $a^x + b^y = p^z$ admet au plus trois solutions.

(vi) Le Maohua en 1993 [Le2]: Soient a, et b deux entiers positifs, sans facteurs carrés et premiers entre eux. Soit h le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-ab})$. Soient m et n des entiers vérifiant $(n, 2h) = 1$. Si $n \geq 8.5 \times 10^6$, alors l'équation

$$ax^2 + 2^{2m}b = y^n,$$

en entiers $x > 0$, $y > 1$, y impair et $(x, y) = 1$ n' a pas de solutions. ■

4. L'équation de Thue. Soient a, b et c des entiers non nuls, premiers entre eux deux à deux. Le théorème de Thue affirme que pour tout $n \geq 3$, l'équation

$$ax^n + by^n = c,$$

n'admet qu'un nombre fini de solutions en entiers x et y. La conjecture abc affirme plus: d'après la preuve de la proposition 15, pour tout triplet (a, b, c) d'entiers premiers entre eux, l'équation ci-dessus n'admet qu'un nombre fini de solutions en entiers x, y et $n \geq 3$. Ceci est confirmé par un théorème de Tijdeman ([Sho-Tij], p. 100) qui établit la finitude du nombre de solutions vérifiant $x > 1$, $y \geq 0$ et $n \geq 3$. ■

5. Une équation en S-entiers. Plus généralement, soient $p_1, \cdots, p_s$ des nombres premiers fixés avec $s \geq 1$. Soit S l'ensemble des entiers formés des nombres premiers p_i, $1 \leq i \leq s$. D'après les théorèmes 2.2 et 12.2 de [Sho-Tij], l'équation:

$$ax^n - by^n = z \tag{16}$$

en entiers $a \in S$, $b \in S$, $z \in S$, $n \geq 3$, $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ n'admet qu'un nombre fini de solutions avec (ax^n, z) borné. La conjecture abc a les mêmes conséquences.

Proposition 33. *La conjecture abc implique que l'équation* (16) *n'a qu'un nombre fini de solutions en entiers $n \geq 3$, $x, y \in \mathbb{Z}$ et $z \in S$.*

Preuve. Supposons que (ax^n, z) soit borné. La proposition 18 montre qu'il n'y a qu'un nombre fini de solutions avec $x = \pm 1$. Supposons alors que $x \neq \pm 1$ et appliquons alors la conjecture abc au triplet (ax^n, by^n, z). On obtient:

$$|x|^n \leq c_1(\varepsilon, p_1, \cdots, p_s)\,(r(xy))^{1+\varepsilon}.$$

Supposons que $|ax^n| > |by^n|$, alors:

$$|y| \leq |ax^n/b|^{1/n} \leq |a|^{1/n}|x|.$$

Maintenant, on a:

$$a|x|^n \leq c_2(\varepsilon, p_1, \cdots, p_s)|a|^{(1+\varepsilon)/n}|x|^{2(1+\varepsilon)},$$

et donc

$$|a|^{1-(1+\varepsilon)/n}|x|^{n-2(1+\varepsilon)} \leq c_2(\varepsilon, p_1, \cdots, p_s),$$

ce qui implique que n est borné et que pour $n \geq 3$, a, x, puis b et y sont bornés. ■

6. Résultats pour l'équation de Pillai. Plusieurs résultats confirment partiellement la proposition conjecturale 15 qui lie la conjecture de Pillai à la conjecture abc:

(i) Stormer en 1899 [Sto2]: L'équation $x^2 + 1 = 2y^n$ n'a aucune solution vérifiant $x > 1$, $y \geq 1$ et $n \geq 3$ impair.

(ii) Pillai en 1931 [Pil]: Soient r, a, s, b et c des entiers donnés. L'équation $ra^x - sb^y = c$ n'admet qu'un nombre fini de solutions en entiers $x > 0$, $y > 0$.

(iii) Ljunggren en 1942 [Lju]: L'équation $x^2 + 1 = 2y^4$ n'a que les deux solutions $(x, y) = (1, 1)$ et $(239, 13)$.

(iv) Nagell en 1960 (cité dans [Mord]): L'équation $x^2 + 7 = 2^n$, n'admet que les cinqs solutions $(x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$.

(v) Cohn en 1964 [Coh1]: L'équation $x^2 - 5y^4 = \pm 4$, $(x, y) = 1$ en entiers positifs n'a que deux solutions $(x, y) = (1, 1), (3, 1)$.

(vi) Zhenfu en 1986 [Zhe]: Soient $n > 2$ et $d > 0$ des entiers avec d non carré parfait et tels que l'équation de Pell $u^2 - dv^2 = -1$ soit solvable. Alors l'équation $x^{2n} - dy^2 = 1$ a pour unique solution $x = 3$, $y = 22$ (lorsque $n = 5$, $d = 122$).

(vii) Le Maohua en 1990 [Le1]: Si p est un nombre premier impair et si d est un entier tel que $d \neq 4p^m - 1$, alors l'équation $x^2 + d = 4p^n$ admet au plus deux solutions (x, n).

(xiii) Cohn en 1992 [Coh2]: L'équation $x^2 + 19 = y^n$ en entiers $x > 1$, $y > 1$, $n \geq 3$ n'admet que les deux solutions $(x, y, n) = (18, 7, 3), (22434, 55, 5)$.

(ix) Scott en 1993 [Sco]: Soient $b > 1$ et $c > 0$ deux entiers donnés et soit p un nombre premier. L'équation $p^x - b^y = c$ a au plus deux solutions en entiers $x > 0$ et $y > 0$. ■

7. Un théorème de Stewart. Soit n un entier positif. On désigne par $P(n)$ le plus grand facteur premier de n. C.L. Stewart [Ste] a montré qu'il existe une constante $c > 0$ effectivement calculable telle que pour tout nombre premier $p > c$ on ait:

$$P(2^p - 1) \geq \frac{p}{2} (\log p)^{1/4}.$$

Ceci implique que $\lim_{p \to +\infty} P(2^p - 1) = +\infty$. La conjecture *abc* permet aussi d'obtenir cette limite. En effet, si on l'applique à la relation $1 + (2^p - 1) = 2^p$, on obtient:

$$2^p \leq c(\varepsilon) \left(r(2^p - 1)\right)^{1+\varepsilon},$$

ce qui montre que $\lim_{p \to +\infty} r(2^p - 1) = +\infty$ et donc que $\lim_{p \to +\infty} P(2^p - 1) = +\infty$. D'autre part, l'inégalité ci-dessus donne:

$$2^p \leq c(\varepsilon) \left(r(2^p - 1)\right)^{1+\varepsilon} \leq c(\varepsilon) 4^{P(2^p - 1)(1+\varepsilon)},$$

ce qui donne:

$$P(2^p - 1) \geq c_1(\varepsilon) p.$$

Cette inégalité est cependant moins bonne que celle de Stewart. ■

8. Un théorème de Shorey. Plus généralement, soient, a, b et $n > 1$ des entiers non nuls. T. N. Shorey [Sho] a montré que pour tous les entiers non nuls x, y, m vérifiant $|x| > 1$, $(ax, by) = 1$ et $m > e^e$, le plus grand facteur premier de $ax^m + by^n$ vérifie:

$$P(ax^m + by^n) \geq c(a, b, n) \left((\log m) (\log \log m)\right)^{1/2},$$

où $c(a, b, n)$ est une constante qui ne dépend que de a, b, et n. Cette inégalité implique que $\lim_{m \to +\infty} P(ax^m + by^n) = +\infty$. Ceci est aussi une conséquence de la conjecture abc, car si on applique celle-ci à la relation suivante, puisque que $(ax^m, by^n) = 1$:

$$ax^m + by^n = z,$$

on obtient, en supposant que $|y^n| < |x^m|$:

$$|x|^m \leq c_1(\varepsilon, a, b)\left(r(xyz)\right)^{1+\varepsilon} \leq c_2(\varepsilon, a, b)|x|^{(1+m/n)(1+\varepsilon)}\left(r(z)\right)^{1+\varepsilon},$$

ce qui donne:

$$\left(|x|^m\right)^{1-\left(n^{-1}+m^{-1}\right)(1+\varepsilon)} \leq c_2(\varepsilon, a, b)\left(r(z)\right)^{1+\varepsilon}.$$

Ceci implique donc aussi que $\lim_{m \to +\infty} P(ax^m + by^n) = +\infty$ lorsque $n > 1$. D'autre part, on a:

$$\left(|x|^m\right)^{1-\left(n^{-1}+m^{-1}\right)(1+\varepsilon)} \leq c_2(\varepsilon, a, b)\left(r(z)\right)^{1+\varepsilon} \leq c_2(\varepsilon, a, b)4^{(1+\varepsilon)P(ax^m+by^n)},$$

ce qui donne:

$$P(ax^m + by^n) \geq c_3(\varepsilon, a, b, n)m.$$

Cette inégalité est meilleure que celle de Shorey. ■

9. La tentative de Wiles. Le 24 juin 1993, A. Wiles a exposé une démonstration du théorème de Fermat, mais actuellement, quelques problèmes non résolus font que le théorème de Fermat reste une conjecture. Le travail de Wiles porte sur la conjecture de Taniyama-Weil. Plus précisement, il a tenté de démontrer la conjecture suivante, en se limitant au cas des courbes elliptiques semi-stables:

Conjecture (Taniyama-Weil). *Toute courbe elliptique E définie sur $\mathbb{Q}$ est modulaire.*

En utilisant les travaux de plusieurs auteurs dont Y. Hellegouarch [Hel1] et G. Frey [Fre] sur les courbes elliptiques E_{abc} définies en 1972 par Y. Hellegouarch (voir aussi la partie II de ce chapitre), K. Ribet a montré en 1987 que si x_1, x_2 et x_3 sont des entiers non nuls vérifiant $x_1^p + x_2^p = x_3^p$ pour un nombre premier $p \geq 5$, alors la courbe elliptique (semi-stable) E définie par:

$$E: \; y^2 = x(x - x_1^p)(x + x_2^p),$$

n'est pas une courbe modulaire, et viole donc la conjecture de Taniyama-Weil sur les courbes elliptiques. Pour plus de détails, on peut consulter par exemple [Oes] et [Fre]. Ainsi, K. Ribet a prouvé le théorème suivant (loc.cit.):

Théorème 12. *La conjecture de Taniyama-Weil implique le théorème de Fermat.*

Maintenant, il est clair comment la tentative de Wiles aurait abouti à la démonstration du théorème de Fermat.

VI. Généralisations de la conjecture abc

1. La conjecture *abc* multidimensionnelle

La conjecture *abc* est une 3-conjecture, c'est-à-dire qu'elle concerne une relation entre trois entiers. Il existe suivant le même principe une n-conjecture *abc*, qui peut être définie comme suit:
Soit $n \geq 3$. Soient $a_1, a_2, \cdots, a_n$ des entiers vérifiant les conditions:

$$(16) \qquad \begin{cases} a_1 + a_2 + \ldots a_n = 0, \\ (a_1, a_2, \cdots, a_n) = 1, \\ \text{Aucune sous-somme n'est nulle.} \end{cases}$$

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:

Conjecture 22. **(n-conjecture *abc*)** *Soit $\varepsilon > 0$. Il existe une constante positive $c(\varepsilon, n)$ ne dépendant que de ε et de n telle que pour tout n-uplet $(a_1, a_2, \cdots, a_n)$ d'entiers vérifiant les conditions* (16), *on ait:*

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

Le n-rapport *abc* peut être défini par:

$$\alpha_n = \frac{\log \max(|a_1|, \cdots, |a_n|}{\log r(a_1 a_2 \cdots a_n)}.$$

Dans [Bro-Brz], J. Browkin et J. Brzezinski ont explicité pour tout $n \geq 3$, une infinité de n-uplets $(a_1, a_2, \cdots, a_n)$ pour lesquels $\alpha_n \geq 2n - 5$.

2. Corps de fonctions

On remarque une certaine similitude entre l'anneau des entiers $\mathbb{Z}$ et l'anneau des polynômes $K[X]$, où K est un corps de caractéristique nulle et il est naturel de se demander si l'analogue de la conjecture *abc* existe dans $K[X]$. En fait, cet analogue existait et avait été démontré par Mason [Mas] avant même la naissance de la conjecture *abc* de Oesterlé-Masser.

Soit $A(X)$ un polynôme à coefficients dans K. On désigne par $r(A)$ le nombre de racines distinctes de A dans une clôture algébrique de K.

Théorème 13. (Mason). *Soient A, B et C trois polynômes de $K[X]$ premiers entre eux, tels que $A+B+C=0$ et dont l'un au moins n'est pas une constante. Alors*

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

Preuve. Supposons que $C' \neq 0$. De l'égalité $A+B+C=0$, on tire $A/C + B/C + 1 = 0$. En dérivant, on obtient:

$$AC' - A'C = CB' - C'B \neq 0.$$

Ainsi, nous avons les inégalités:

$$-\infty < \deg(AC' - A'C) \leq \deg(A) + \deg(C) - 1 \tag{17}$$

Soit θ une racine de A, de multiplicité $n \geq 1$ dans une clôture algébrique de K. Alors

$$A(X) = (X-\theta)^n a(X),$$

où a est un polynôme tel que $a(\theta) \neq 0$. Alors

$$(AC' - A'C)(X) = (X-\theta)^{n-1}\Big((X-\theta)(aC' - a'C)(X) - n(aC)(X)\Big),$$

ce qui donne:

$$\deg(AC' - A'C) \geq n - 1,$$

puisque $AC' - A'C \neq 0$. En considérant les $r(ABC)$ racines distinctes de ABC, on obtient:

$$\deg(AC' - A'C) \geq \deg(A) + \deg(B) + \deg(C) - r(ABC),$$

et en comparant avec l'inégalité (17), on obtient $\deg(B) \leq r(ABC) - 1$. On conclut en utilisant la symétrie de l'équation. ■

Quelques exemples particuliers montrent qu'on peut avoir une égalité dans le théorème de Mason. Les exemples suivants sont tirés de l'égalité $c_4^3 - c_6^2 = 1728\Delta$ où c_4, c_6 et Δ sont des invariants associés à des courbes elliptiques. On pose:

$$\begin{aligned}
A(X) &= 1 + X + X^2, \\
B(X) &= 2(1+2X)(X-1)(2+X), \\
C(X) &= 1728X^2(1+X)^2.
\end{aligned}$$

Ces polynômes proviennent des courbes E_{abc} définies par (1). Le triplet $(A^3, -B^2, -C)$ représente un cas d'égalité pour le théorème de Mason. On pose maintenant:

$$\begin{aligned}
A(X) &= (1 - X + X^2)(1 - 11X + 30X^2 - 15X^3 - 10X^4 + 5X^5 + X^6),\\
B(X) &= -X^{12} - 6X^{11} + 15X^{10} + 46X^9 - 174X^8 + 222X^7\\
&\quad - 273X^6 + 486X^5 - 570X^4 + 354X^3 - 117X^2 + 18X - 1,\\
C(X) &= 1728X^7(1 - X)^7(1 - 8X + 5X^2 + X^3),\\
D(X) &= (1 - X + X^2)(1 + 229X + 270X^2 - 1695X^3 + 1430X^4 - 235X^5 + X^6),\\
E(X) &= -X^{12} - 510X^{11} + 14631X^{10} - 80090X^9 + 218058X^8 - 316290X^7\\
&\quad + 253239X^6 - 131562X^5 + 70998X^4 - 37950X^3 + 8955X^2 + 522X - 1,\\
F(X) &= 1728X(1 - X)(1 - 8X + 5X^2 + X^3)^7.
\end{aligned}$$

Ces polynômes sont issus des courbes elliptiques définies dans la partie III du chapitre 2. Alors les triplets $(A^3, -B^2, -C)$ et $(D^3, -E^2, -F)$ vérifient l'égalité du théorème de Mason.

L'exemple suivant est dû à Birch (Voir [Lan]):

$$\begin{aligned}
a(X) &= X^6 + 4X^4 + 10X^2 + 6,\\
b(X) &= X^9 + 6X^7 + 21X^5 + 35X^3 + \frac{63}{2}X.
\end{aligned}$$

Soient $A = a^3$, $B = b^2$ et $C = A - B$. Alors:

$$18 = \deg(A) = \deg(B) = r(ABC) - 1.$$

D'autre part, M. Langevin a explicité dans [Lange2] une infinité de familles de polynômes A, B et C vérifiant $(A, B, C) = 1$, $A+B+C = 0$ et tels que $\max(\deg(A), \deg(B), \deg(C)) = r(ABC) - 1$. En voici quelques exemples:

(i) $A(X) = (X - n)^m(X + m)^n$, $B(X) = (X - m)^n(X + n)^m$, $C = A - B$, m, n entiers positifs.

(ii) $A(X) = (X^2 - m^2)^{n^2}$, $B(X) = X^{2(n^2 - m^2)}(X^2 - n^2)^{m^2}$, $C = A - B$, m, n entiers.

(iii) Soit $k \geq 2$ un entier fixé. On définit les entiers m_i et n_i, $1 \leq i \leq k$ par:

$$\begin{cases} m_i = \binom{k-1}{i-1}, n_i = 0 \text{ si } i \text{ est pair},\\ m_i = 0, n_i = \binom{k-1}{i-1} \text{ si } i \text{ est impair.}\end{cases}$$

Soient $A_k(X) = \prod_{i=1}^k (X + i)^{m_i}$, $B_k(X) = \prod_{i=1}^k (X + i)^{n_i}$, et $C_k = A_k - B_k$. Alors $\deg(A_k) = 2^{k-2}$, $\deg(B) = 2^{k-2}$, $\deg(C) = 2^{k-2} - k + 1$, $r(A_kB_kC_k) = 2^{k-2} + 1$ ce qui donne $\deg(A_k) = \deg(B_k) = r(A_k B_k C_k) - 1$. Cette famille est doublement intéressante car le nombre de racines distinctes de $A_k B_k C_k$ peut être arbitrairement grand, ainsi que les degrés des trois polynômes.

Le théorème de Mason est très utile pour l'étude des équations diophantiennes polynômiales. Nous ne nous étendrons pas sur ce sujet. Signalons seulement le résultat suivant.

Proposition 34. *Soient a, b et c trois polynômes premiers entre eux deux à deux. L'équation:*

$$a(X)P(X)^l + b(X)Q(X)^m = c(X)R(X)^n,$$

en polynômes non constants P, Q et R tels que aP et bQ soient premiers entre eux et en entiers $l \geq 3$, $m \geq 3$, $n \geq 3$ avec $lmn \geq 48$ n'admet que des solutions telles que $\deg(P)$, $\deg(Q)$, $\deg(R)$, *l, m et n sont bornés.*

Preuve. Le théorème de Mason implique:

$$\begin{aligned}\deg(a) + l\deg(P) + \deg(b) + m\deg(Q) + \deg(c) + n\deg(R) \\ &\leq 3\deg(abcPQR) - 3 \\ &\leq 3\left(\deg(a) + \deg(P) + \deg(b) + \deg(Q) + \deg(c) + \deg(R)\right) - 3,\end{aligned}$$

d'où l'on tire:

$$(l-3)\deg(P) + (m-3)\deg(Q) + (n-3)\deg(R) \leq 2(\deg(a) + \deg(b) + \deg(c)) - 3.$$

Ceci montre d'une part que les exposants l, m et n sont bornés et d'autre part que pour $l \geq 3$, $m \geq 3$ et $n \geq 3$, avec $lmn \geq 48 (= 3 \times 4 \times 4)$, les degrés de Q et de R sont bornés et donc celui de P aussi. ∎

Remarque. Un cas particulier important est si $\deg(a) + \deg(b) + \deg(c)) \leq 1$, alors on ne peut pas avoir en même temps $l \geq 3$, $m \geq 3$ et $n \geq 3$, c'est le cas par exemple pour l'équation de Fermat:

$$P(X)^n + Q(X)^n = R(X)^n,$$

qui n'admet donc pas de solutions pour $n \geq 3$.

3. Corps de nombres

Soit K un corps de nombres. Soit E/K une courbe elliptique définie par une forme normale de Weierstrass sur K. Soient $\Delta_{E/K}$ l'idéal discriminant minimal de E/K et $F_{E/K}$ son idéal conducteur. On définit le quotient de Szpiro de E sur K par:

$$\sigma_{E/K} = \frac{\log N_{K/\mathbb{Q}}\left(\Delta_{E/K}\right)}{\log N_{K/\mathbb{Q}}\left(F_{E/K}\right)},$$

avec par convention $\sigma_E = 1$ si $N_{K/\mathbb{Q}}(F_{E/K}) = 1$. La conjecture de Szpiro dans K est (voir par exemple [Fre]):

Conjecture 23. (Szpiro). *Pour tout nombre réel $d > 1$, il existe une constante $c(d, K)$ ne dépendant que de d et de K telle que pour toute courbe elliptique E sur K, le quotient de Szpiro est majoré par:*

$$\sigma_{E/K} \leq 6d + \frac{c(d, K)}{\log N_{K/Q}(F_{E/K})}.$$

La conjecture abc sur K quant à elle peut être formulée ainsi:

Conjecture 24. (abc). *Pour tout nombre réel $d > 1$, il existe une constante $C(d, K)$ telle que pour tout triplet (a, b, c) d'entiers de l'anneau de K vérifiant $(a, b, c) = 1$ et $a+b+c = 0$, on ait:*

$$\log \max \Big(N_{K/\mathbb{Q}}(a), N_{K/\mathbb{Q}}(b), N_{K/\mathbb{Q}}(c)\Big) \leq C(d, K) + d \log N_{K/\mathbb{Q}}(r(abc)),$$

où $r(abc)$ désigne le produit des idéaux premiers divisant abc.

Le quotient abc d'une relation $a + b + c = 0$ entre entiers premiers entre eux est défini par:

$$\alpha_{K/\mathbb{Q}}(a, b, c) = \frac{\log \max \Big(N_{K/\mathbb{Q}}(a), N_{K/\mathbb{Q}}(b), N_{K/\mathbb{Q}}(c)\Big)}{\log N_{K/\mathbb{Q}}(r(abc))}.$$

Signalons l'existence d'une conjecture de G. Frey sur les hauteurs des courbes elliptiques sur un corps de nombres. Frey affirme que cette conjecture est équivalente à la conjecture abc et implique donc la conjecture 23 de Szpiro (voir [Fre]). Pour une courbe elliptique E définie sur K, on définit sa hauteur globale $h_K(E)$ par:

$$h_K(E) = \frac{1}{12} \max \Big(\log N_{K/\mathbb{Q}}(\Delta_{E/K}), \log N_{K/\mathbb{Q}}(j_{E/K})\Big),$$

où $j_{E/K}$ désigne le j-invariant de E (voir appendice A).

Conjecture 25. (Frey). *Il existe un nombre réel d et une constante $c(d, K)$ ne dépendant que de d et de K tels que pour toute courbe elliptique E sur K, de conducteur $F_{E/K}$, la hauteur globale $h_K(E)$ de E est majorée par:*

$$h_K(E) \leq c(d, K) + \frac{d}{2} \log N_{K/\mathbb{Q}}(F_{E/K}).$$

CHAPITRE 2

Les équations de Thue et de Pell

I. L'équation de Thue

II. L'équation de Pell et l'algorithme de Cornacchia

III. Application des équations de Thue

Les équations de Thue et de Pell

I. L'équation de Thue

Soit $f(x,y)$ un polynôme homogène, irréductible sur $\mathbb{Q}$, de degré n à coefficients dans $\mathbb{Z}$. Soit m un entier non nul. L'équation

$$f(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i = m \tag{1}$$

en entiers x et y est appelée équation de Pell si $n = 2$ et équation de Thue si $n \geq 3$.
Lorsque $n \geq 3$, cette équation n'admet qu'un nombre fini de solutions (théorème de Thue) contrairement au cas $n = 2$ où elle peut en avoir une infinité. En 1968, A. Baker [Bak] a explicité une borne pour les solutions de cette équation lorsque $n \geq 3$:

$$\max(|x|,|y|) < \exp\left(n^{\nu^2} H^{\nu n^3} + (\log|m|)^{2n+2}\right),$$

où $\nu = 128n(n+1)$ et $H = \max|a_i|$. Cette borne est encore trop grande pour qu'elle soit effectivement utilisable sur les machines actuelles.
Si (x,y) est une solution de (1) où y est négatif, alors on peut écrire:

$$\sum_{i=0}^{n} a_i(-x)^{n-i}(-y)^i = (-1)^n m.$$

On peut donc remplacer l'équation (1) par l'équation $f(x,y) = \pm m$ en entiers $x \neq 0$ et $y > 0$. Dans la suite, on supposera que $m > 0$ et on ne cherchera que les solutions (x,y) vérifiant $y > 0$ et $(y,m) = 1$. Cette équation devient donc le cas particulier $z = \pm 1$ de l'équation:

$$f(x,y) = \sum_{i=0}^{n} a_i x^{n-i} y^i = mz \tag{2}$$

en entiers x, y, z où $y > 0$, $(y,m) = 1$ et $z \neq 0$. On considère la congruence qui lui est attachée:

$$\sum_{i=0}^{n} a_i t^{n-i} \equiv 0 \pmod{m} \tag{3}$$

avec $0 \leq |t| \leq m/2$. Le lemme suivant détermine le lien entre la congruence (3) et l'équation (2).

Lemme 1. *L'équation (2) a une solution (x,y,z) telle que $(m,y)=1$ si et seulement si la congruence (3) a une solution t vérifiant $0 \leq |t| \leq m/2$. Si (x,y,z) est une solution de (2) avec $(m,y)=1$, alors $t \equiv xy^{-1} \pmod m$ avec $0 \leq |t| \leq m/2$ est une solution de (3) et il existe un entier u tel que $x = ty - mu$.*

Preuve. Si (x,y,z) est une solution de (2) avec $(m,y)=1$ et si $t \equiv xy^{-1} \pmod m$, avec $0 \leq |t| \leq m/2$, alors t est une solution de (3). De plus, il existe un entier u tel que $x = ty - mu$.
Inversement, si t est une solution de (3), alors il existe un entier q tel que $f(t,1) = mq$ et donc $(t,1,q)$ est une solution de (2). De plus, si u et v avec $(v,m)=1$ sont deux entiers quelconques, alors:

$$f(tv - mu, v) \equiv v^n \sum_{i=0}^{n} a_i t^{n-i} \equiv 0 \pmod m,$$

et donc $(tv - mu, v, f(tv-mu,v)/m)$ est une autre solution de (2). ■

On pose $g(x) = f(x,1)$ pour tout $x \in \mathbb{C}$. Puisque f est irréductible sur $\mathbb{Q}$, l'équation $g(\theta) = 0$ a n racines distinctes dans $\mathbb{C}$. On les note θ_i $(i = 1, \ldots, n)$.

Théorème 1. *Soit $(x,y,\pm 1)$ une solution de (2) avec $y \geq 1$ et $(m,y)=1$. Soit $t \equiv xy^{-1} \pmod m$, $0 \leq |t| \leq m/2$. Soit θ_{i_0} une racine vérifiant $|x - y\theta_{i_0}| = \min_{1 \leq i \leq n} |x - y\theta_i|$. On pose:*

$$V_0(\theta_{i_0}) = \left(\frac{2^{n-1} m}{|g'(\theta_{i_0}) Im(\theta_{i_0})|} \right)^{1/n} \qquad si \;\; \theta_{i_0} \in \mathbb{C} - \mathbb{R},$$

$$V_1(\theta_{i_0}) = \left(\frac{2^n}{|g'(\theta_{i_0})|} \right)^{1/(n-2)} \qquad si \;\; n \geq 3 \;,$$

$$\Delta = a_1^2 - 4a_0 a_2 \qquad si \;\; n = 2 \;.$$

Alors on a les deux propriétés suivantes:
(i) Si $\theta_{i_0} \in \mathbb{C} - \mathbb{R}$ alors $y \leq V_0(\theta_{i_0})$.
(ii) Si $n \geq 3$ et $y \geq V_1(\theta_{i_0})$ ou si $n = 2$ et $|\Delta| \geq 16$, alors il existe une réduite u/v de la fraction continue de $\dfrac{t - \Re e\,(\theta_{i_0})}{m}$ telle que $x = tv - mu$ et $y = v$.

Preuve. D'après la définition de i_0, on a:

$$\prod_{i \neq i_0} \left| \frac{x}{y} - \theta_i \right| \geq \frac{1}{2^{n-1}} \prod_{i \neq i_0} \left(\left| \frac{x}{y} - \theta_{i_0} \right| + \left| \frac{x}{y} - \theta_i \right| \right) \geq \frac{1}{2^{n-1}} \prod_{i \neq i_0} |\theta_{i_0} - \theta_i| = \frac{|g'(\theta_{i_0})|}{2^{n-1}|a_0|} \;.$$

On obtient alors:

$$(4) \qquad \left|\frac{x}{y}-\theta_{i_0}\right| = \frac{m}{\left|a_0 \prod_{i\neq i_0}(x/y-\theta_i)\right| y^n} \leq \frac{2^{n-1}m}{|g'(\theta_{i_0})|y^n} \ .$$

(i) Si $\theta_{i_0} \in \mathbb{C} - \mathbb{R}$, alors:

$$|Im(\theta_{i_0})| \leq \left|\frac{x}{y}-\theta_{i_0}\right| \leq \left(\frac{V_0(\theta_{i_0})}{y}\right)^n |Im(\theta_{i_0})| \ ,$$

ce qui implique que $y \leq V_0(\theta_{i_0})$.
(ii) La relation (4) donne aussi:

$$\left|\frac{x}{y} - \Re e\,(\theta_{i_0})\right| \leq \frac{2^{n-1}m}{|g'(\theta_{i_0})|y^n} \ .$$

Soit $t \equiv xy^{-1} \pmod m$. Soient u et v tels que $y = v$ et $x = tv - mu$. Alors:

$$\left|\frac{u}{v} - \frac{t-\Re e\,(\theta_{i_0})}{m}\right| \leq \begin{cases} \left(\frac{V_1(\theta_{i_0})}{v}\right)^{n-2} \frac{1}{2v^2} & \text{si } n \geq 3, \\ \frac{2}{\sqrt{|\Delta|}v^2} & \text{si } n = 2. \end{cases}$$

Ainsi, si $n \geq 3$ et $y \geq V_1(\theta_{i_0})$ ou si $n = 2$ et $|\Delta| \geq 16$, alors, d'après le théorème 2 de l'annexe B, u/v est une réduite de la fraction continue de $\frac{t-\Re e\,(\theta_{i_0})}{m}$. ■

Remarques

(i) D'après le théorème de Roth, l'inégalité (4) implique, lorsque $n \geq 3$, que l'equation (1) ne peut admettre qu'un nombre fini de solutions. Ce résultat est l'un des théorèmes de Thue.

(ii) Le théorème 1 donne une borne inférieure pour y, indépendante de m, pour que (x, y) provienne d'une réduite d'une fraction continue d'un certain nombre $\frac{t-\Re e\,(\theta_i)}{m}$ où t est une solution de la congruence (3) et où θ_i est une solution de l'équation $g(\theta) = 0$, mais il ne permet pas de déterminer toutes les solutions de l'équation (1) lorsque $n \geq 3$ car on ne connait pas une borne supérieure accessible dans la pratique pour les solutions. De nombreuses méthodes permettent cependant de déterminer toutes les solutions de l'équation (1), mais elles sont plus coûteuses: il faut disposer d'un système d'unités fondamentales du corps $\mathbb{Q}\,(\theta)$, où θ est une solution de l'équation $g(x) = 0$. Les méthodes de Gelfond-Baker sur les formes linéaires de logarithmes permettent de trouver une borne pour les solutions.

On peut ensuite réduire cette borne en utilisant par exemple l'analogue p-adique, dû à B.M.M. de Weger, de l'algorithme L^3 de Lenstra, Lenstra et Lovasz. Pour plus de details, on peut consulter par exemple le livre de B.M.M de Weger [Weg].
Dans la partie III de ce même chapitre, nous verrons quelques applications de la résolution des équations de Thue.

II. L'équation de Pell et l'algorithme de Cornacchia

Soient $a > 0$, $b \neq 0$, $m \neq 0$ des entiers non nuls premiers entre eux deux à deux. Dans cette partie, on présente deux algorithmes pour résoudre des équations de Pell:

$$ax^2 - by^2 = m,$$

en entiers x et y avec $y > 0$ et $(x, y) = 1$. On supposera le long de cette partie que a, b et m sont tels que la congruence

$$at^2 - b \equiv 0 \pmod{m},$$

soit résoluble. Si ce n'est pas le cas, on peut toujours s'y ramener en simplifiant m par des carrés s^2 tels que $s^2|m$. La proposition suivante lie la congruence ci-dessus à l'équation de Pell.

Proposition 1. *Soient $a > 0$, $b \neq 0$ et m des entiers premiers entre eux deux à deux. Si la congruence $at^2 - b \equiv 0 \pmod{m}$, est résoluble, alors toute solution (x, y) de l'équation $ax^2 - by^2 = m$, vérifie $(x, y) = 1$, $(x, m) = 1$ et $(y, m) = 1$.*

Preuve. Soit (x, y) une solution de l'équation $ax^2 - by^2 = m$. D'après le lemme 1, il existe une solution t de la congruence $at^2 - b \equiv 0 \pmod{m}$ avec $0 \leq |t| \leq |m|/2$ et deux entiers u et v tels que $x = tv - mu$ et $y = v$. Soit q tel que $at^2 - b = mq$, alors:

$$ax^2 - by^2 = a(tv - mu)^2 - bv^2 = m(qv^2 - 2atuv + amu^2) = m,$$

et donc $qv^2 - 2atuv + amu^2 = 1$. Cette dernière égalité implique donc que $(u, v) = 1$ et $(v, m) = 1$. Ainsi, on a $(y, m) = 1$ et par suite $(x, m) = 1$ et $(x, y) = 1$. ■

Les algorithmes que nous allons décrire comportent deux phases: résolution de la congruence $at^2 - b \equiv 0 \pmod{m}$ attachée à à l'équation de Pell $ax^2 - by^2 = m$, puis calcul de réduites du dévelopement en fraction continue de certains nombres réels. Commençons par étudier la congruence.

1. Résolution de la congruence $at^2 - b \equiv 0 \pmod{m}$

Soient $a > 0$, $b \neq 0$ et $m > 0$ des entiers premiers entre eux deux à deux. Nous allons commencer par étudier la congruence

$$at^2 - b \equiv 0 \pmod{m},$$

avec $0 \leq t \leq m/2$. Puisque $(a, m) = 1$, alors ba^{-1} existe modulo m et en posant $d \equiv ba^{-1} \pmod{m}$, on est ramené à étudier la nouvelle congruence:

$$t^2 \equiv d \pmod{m}, \tag{5}$$

avec $0 \leq |t| < m/2$. L'égalité $t = 0$ ne se produit que si $m = 1$. Ecartons ce cas et écrivons m sous forme de produit de facteurs premiers:

$$m = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

avec $e_0 = 0$ si m est impair, $e_0 \geq 1$ si m est pair, $e_i \geq 1$ pour $1 \leq i \leq r$ et $3 \leq p_1 < \ldots < p_r$ où chaque p_i est un nombre premier. La congruence (5) est alors équivalente au système suivant:

$$\begin{cases} t^2 \equiv d \pmod{2^{e_0}}, \\ t^2 \equiv d \pmod{p_i^{e_i}} \quad 1 \leq i \leq r. \end{cases}$$

On peut donc résoudre séparément ces r (si $e_0 = 0$) ou ces $r + 1$ (si $e_0 \geq 1$) équations et utiliser le théorème des restes chinois pour déterminer les solutions de (5).

a. Résolution de la congruence $t^2 \equiv d \pmod{2^{e_0}}$

On cherche les solutions t de la congruence:

$$t^2 \equiv d \pmod{2^{e_0}}, \tag{6}$$

tels que $0 < |t| \leq 2^{e_0 - 1}$. On suppose donc que $e_0 \geq 1$ et que d est impair. On distingue les cas suivants :

- Si $e_0 = 1$, alors $d \equiv 1 \pmod{2}$, et donc $t = 1$.
- Si $e_0 = 2$, alors $d \equiv 1 \pmod{4}$ ou $d \equiv 3 \pmod{4}$. Si $d \equiv 1 \pmod{4}$, alors $t = \pm 1$. Si $d \equiv 3 \pmod{4}$ la congruence (6) n'admet pas de solution.
- Si $e_0 \geq 3$, alors toute solution t de (6) avec $0 < t < 2^{e_0 - 1}$ vérifie $t^2 \equiv d \pmod{8}$. Si $d \not\equiv 1 \pmod{8}$, alors il n'y a pas de solution, et donc (6) n'admet pas de solution. Si $d \equiv 1 \pmod{8}$, il y a quatre solutions t telles que $t \equiv \pm 1, \pm 3 \pmod{8}$. On peut ensuite déterminer une solution de la congruence (6) avec $0 < t < 2^{e_0 - 1}$ en appliquant la méthode de Newton pour la résolution des équations dans les corps complets. Ici, il

s'agit de $\mathbb{Q}_2$, corps des nombres 2-adiques (voir [Bac] p. 52). Le lemme de Hensel garantit la convergence de cette méthode. Connaissant une solution t, $0 < t < 2^{e_0-1}$, on peut déterminer les trois autres solutions pour la congruence (6) en prenant $-t$, $\pm(2^{e_0-1} - t)$. La méthode de Newton consiste à définir une suite $a_3, a_4, \cdots, a_{e_0}$ de la manière suivante:

$$\begin{cases} a_3 = 1, \\ a_{k+1} \equiv a_k - \dfrac{(a_k^2 - d)}{2} \pmod{2^k}, \quad 3 \leq k \leq e_0 - 1, \quad 0 < a_{k+1} < 2^k. \end{cases}$$

Alors une solution de la congruence (6) est $t = a_{e_0}$. Sachant que $0 < a_{e_0} < 2^{e_0-1}$, les autres solutions sont $-a_{e_0}$, et $\pm(2^{e_0-1} - a_{e_0})$.

b. Résolution de la congruence $t^2 \equiv d \pmod{p_i^{e_i}}$, p_i premier impair

Pour $e_i \geq 1$ et p_i premier impair, on veut maintenant résoudre la congruence:

$$t^2 \equiv d \pmod{p_i^{e_i}} \tag{7}$$

avec $0 < |t| < p_i^{e_i}/2$. Toute solution de cette congruence vérifie:

$$t^2 \equiv d \pmod{p_i}. \tag{8}$$

Cette dernière congruence n'admet de solution que si d est un résidu quadratique modulo p_i. On peut donc utiliser le symbole de Legendre:
- Si $\left(\frac{d}{p_i}\right) = -1$, la congruence (8) n'a pas de solution et donc (7) n'a pas de solution.
- Si $\left(\frac{d}{p_i}\right) = 1$, la congruence (7) admet exactement deux solutions t vérifiant $0 < |t| < p_i^{e_i}/2$.
Mettons-nous dans le cas où la congruence (8) a des solutions. Si $p_i \equiv 3 \pmod 4$, alors les solutions de cette congruence sont:

$$t \equiv \pm d^{(p_i+1)/4} \pmod{p_i}, \qquad 0 < |t| < p_i/2.$$

Si $p_i \not\equiv 3 \pmod 4$, on peut utiliser l'algorithme Ressol décrit en appendice C pour déterminer une solution de la congruence (8).
Supposons maintenant qu'une solution $t_{i,1}$ de cette congruence est connue. Le lemme de Hensel et la méthode de Newton, appliqués dans le corps p-adique $\mathbb{Q}_{p_i}$, permettent alors de déterminer une solution de la congruence (7), en définissant une suite $a_1, a_2, \cdots, a_{e_i}$ de la façon suivante:

$$\begin{cases} a_1 = t_{i,1}, \\ a_{k+1} \equiv a_k - (2a_k)^{-1}(a_k^2 - d) \pmod{p_i^{k+1}}, \quad 1 \leq k \leq e_i - 1, \quad 0 < |a_{k+1}| < p_i^{k+1}/2, \end{cases}$$

où $(2a_k)^{-1}$ est l'inverse a' de $2a_k$ modulo p_i vérifiant $0 < a' < p_i$. Alors les deux solutions de la congruence (8) sont $t = \pm a_{e_i}$.

c. Nombres de solutions de la congruence $t^2 \equiv d \pmod m$

Supposons que la congruence (6) a une solution t_0 avec $0 < t_0 < 2^{e_0 - 1}$ et les congruences (7) ont des solutions t_i avec $0 < t_i < p_i^{e_i}$. Toutes les solutions de la congruence (5) peuvent être déterminées en appliquant le théorème des restes chinois au système suivant:

$$\text{(9)} \qquad \begin{cases} t \equiv \pm t_0, \pm(2^{e_0-1} - t_0) \pmod{2^{e_0}}, \\ t \equiv \pm t_i \pmod{p_i^{e_i}},\ 1 \leq i \leq r, \end{cases}$$

avec $0 < |t| < m/2$. On distingue quatre possibilités suivant les valeurs de e_0:
- Si $e_0 = 0$, alors le système (9) et donc la congruence (5) admettent 2^r solutions.
- Si $e_0 = 1$, alors la congruence (6) n'a qu'une solution et donc le système (9) et la congruence (5) admettent 2^r solutions.
- Si $e_0 = 2$, alors la congruence (6) a deux solutions et donc le système (9) et la congruence (5) admettent 2^{r+1} solutions.
- Si $e_0 \geq 3$, la congruence (6) a quatre solutions et donc le système (9) et la congruence (5) admettent 2^{r+2} solutions. ■

2. L'algorithme de Cornacchia

Soient a, b et c des entiers strictement positifs, premiers entre eux deux à deux et tels que $m > 2$. On considère l'équation:

$$\text{(10)} \qquad ax^2 + by^2 = m,$$

en entiers $x \neq 0$, $y > 0$ et tels que $(y, m) = 1$ et la congruence:

$$\text{(11)} \qquad t^2 \equiv -ba^{-1} \pmod m,$$

avec $0 < |t| < m/2$.

Dans cette partie, nous donnons une nouvelle démonstration de l'algorithme de Cornacchia, qui date de 1908 (voir [Cor]) et qui permet de déterminer les solutions de l'équation (10). Cette démonstration se distingue particulièrement par sa simplicité de celles qui sont décrites récemment dans [Ha-Mu-Wi] et [Mor]. Voici une description de l'algorithme de Cornacchia.

Résoudre la congruence $t^2 \equiv ba^{-1} \pmod{m}$. *Pour chaque solution* t *avec* $0 < t < m/2$, *appliquer l'algorithme d'Euclide à* t *et* m *et déterminer le premier reste* $r < \sqrt{m/a}$. *Alors s'il ya une solution pour l'équation* (10), *elle est de la forme* $\left(r, \sqrt{(m - ar^2)/b}\right)$.

a. Résolution de l'équation $ax^2 + by^2 = m$

Le théorème 1 a pour conséquence le corollaire suivant, dont nous donnons une autre preuve, plus directe.

Corollaire 1. *Toute solution* (x, y) *de l'équation* (10) *vérifiant* $x \neq 0$, $y > 0$ *et* $(y, m) = 1$ *provient d'une réduite de la fraction continue de* t/m *où* t *est tel que* $t \equiv xy^{-1} \pmod{m}$ *et* $0 < |t| < m/2$.

Preuve. Soit (x, y) une solution de l'équation (10). Soit t tel que $t \equiv xy^{-1} \pmod{m}$ et $0 < |t| < m/2$. Le lemme 1 implique qu'il existe deux entiers u et v tels que $y = v$ et $x = tv - mu$. Puisque $2|x|y < ax^2 + by^2 = m$, alors:

$$\left|\frac{u}{v} - \frac{t}{m}\right| = \frac{|x|}{mv} \leq \frac{1}{2v^2}.$$

Il en résulte alors, d'après le théorème 2 de l'appendice B que u/v est une réduite de t/m. ■

La proposition suivante montre qu'une solution t de la congruence (11) donne au plus une solution pour l'équation (10), et donc que le nombre de solutions de cette équation est au plus égal au nombre de solutions de la congruence (11).

Proposition 2. *Soit* t *une solution de la congruence* (11). *Si* (x, y) *et* (x', y') *sont deux solutions de l'équation* (10) *vérifiant* $x \equiv ty \pmod{m}$ *et* $x' \equiv ty' \pmod{m}$, *alors* $x = x'$ *et* $y = y'$.

Preuve. Des congruences $x \equiv ty \pmod{m}$ et $x' \equiv ty' \pmod{m}$, on tire:

$$axx' + byy' \equiv (at^2 + b)yy' \equiv 0 \pmod{m},$$

et donc $axx' + byy' = mq_1$. On a de même $xy' - yx' \equiv 0 \pmod{m}$ et donc $xy' - yx' = mq_2$. Des égalités $ax^2 + by^2 = m$, et $ax'^2 + by'^2 = m$, on tire:

$$(axx' + byy')^2 + ab(xy' - yx')^2 = m^2,$$

ce qui donne:

$$q_1^2 + abq_2^2 = 1,$$

et donc $q_2 = 0$. Alors $x/y = x'/y'$, ce qui donne $x = x'$ et $y = y'$ puisque $y > 0$, $y' > 0$, $(x, y) = 1$ et $(x', y') = 1$. ■

Nous donnons maintenant la démonstration de l'algorithme de Cornacchia. Nous dirons qu'une solution t de la congruence (11) produit une solution s'il existe une réduite u/v de t/m telle que (x, y) est une solution de l'équation (10) avec $x = tv - mu$ et $y = v$.

Théorème 2. *Soit t une solution de la congruence* (11) *avec $0 < |t| < m/2$. Soient u_i/v_i, $i = -2, -1, \cdots$ les réduites de t/m. Si t produit une solution (x_k, y_k) pour l'équation* (10), *avec $x_k = tv_k - mu_k$ et $y_k = v_k$, alors k est le plus petit entier $i \geq 0$ tel que $|x_i| \leq \sqrt{m/a}$.*

Preuve. Si une solution t de la congruence (11) produit une solution, alors d'après le corollaire 1, elle est de la forme $x_k = tv_k - mu_k$, $y_k = v_k$ où u_k/v_k est une réduite de t/m, avec $k \geq 0$. On a alors:

$$|x_k| \leq \sqrt{m/a}.$$

On sait (voir [Ni-Zu-Mo]) que la suite $(u_i/v_i)_{i \geq 0}$ des réduites de t/m vérifie pour tout $i \geq 1$:

$$|tv_i - mu_i| < |tv_{i-1} - mv_{i-1}| \quad \text{et} \quad y_{i-1} \leq y_i.$$

Soit $i_0 \geq 0$ le plus petit entier tel que $|x_{i_0}| \leq \sqrt{m/a}$. Si $i_0 < k$, alors $y_{i_0} \leq y_k$ et donc (x_{i_0}, y_{i_0}) est aussi une solution de l'équation (10) produite par t, ce qui n'est pas possible d'après la proposition 2. ■

Pour résoudre l'équation (10), il suffit donc de développer les différents rationnels t/m en fraction continue, où t décrit l'ensemble des solutions de la congruence (11). Le lemme suivant montre qu'il suffit de considérer uniquement les solutions t tels que $0 < -t < m/2$.

Lemme 2. *Soit t, $0 < t < m/2$, une solution de la congruence* (11). *Toute convergente de t/m est l'opposée d'une convergente de $-t/m$.*

Preuve. Développons t/m en fraction continue, $t/m = [a_0, a_1, a_2, \ldots, a_k]$ avec $a_k \geq 2$. On a $a_0 = [t/m] = 0$ et $a_1 = [m/t] \geq 2$. Alors

$$-t/m = [-1, 1, a_1 - 1, a_2, a_3, \ldots, a_k].$$

Soient u_i/v_i et u'_i/v'_i, $i = -2, -1, \ldots$ les réduites de t/m et $-t/m$ respectivement. Alors il est simple de montrer que pour tout $i \geq 1$, $u'_i = -u_{i-1}$ et $v'_i = v_{i-1}$. ■

Remarque. Le lemme 2 montre que nous aurons à développer en fraction continue uniquement les rationnels $-t/m$ avec $0 < t < m/2$. En effet, si u/v est une réduite de t/m, alors $-u/v$ est une réduite de $-t/m$ et si (x, y) est une solution produite par t, alors $|x| = |tv - mu| = |-tv + mu|$. Ceci signifie que toute solution produite par t peut être produite par $-t$, à un signe près.

Nous donnons maintenant un algorithme pour résoudre complètement l'équation (10).

b. Algorithme 1. $(ax^2 + by^2 = m)$

Entrée: $a > 0$, $b > 0$, $m = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$.

Initialisation: Déterminer les solutions t_j, $j = 1, \cdots, n_0$ de $t^2 \equiv -ba^{-1} \pmod{m}$ telles que $0 < t_j < m/2$;

$j := 0$;
Tant que $j \leq n_0 - 1$ **répéter**
    $j := j + 1$;
    $y_{-1} := 0$;
    $i := -1$;
    $q := 0$;
    Tant que $y_i < \sqrt{m/b}$ **et** $q \neq 1$ **répéter**
        $i := i + 1$;
        Calculer la réduite $\dfrac{u_i}{y_i}$ de $-\dfrac{t_j}{m}$;
        $x_i := t_j y_i + m u_i$;
        Si $|x_i| \leq \sqrt{m/a}$ **alors**
            $q := (ax_i^2 + by_i^2)/m$;
            Si $q = 1$ **alors** écrire x_i et y_i;

Sortie: x et y tels que $ax^2 + by^2 = m$. ∎

c. Complexité de l'algorithme 1

Nous allons maintenant déterminer la complexité de l'algorithme 1.

Théorème 3. *Si la factorisation de m est donnée et si pour chaque nombre premier p divisant m, un non-résidu quadratique modulo p est connu, alors l'algorithme 1 détermine une solution pour l'équation (10) en:*

$$O\left(\log^2 m\right).$$

Preuve. Dans cet algorithme, nous supposons que la factorisation de m est donnée. Dans la phase d'initialisation, le calcul de $a^{-1} \pmod m$ se fait par l'algorithme d'Euclide en:

$$O(\log m).$$

Posons $d \equiv -ba^{-1} \pmod m$. Pour chaque nombre premier impair p_i, $1 \leq i \leq r$, le calcul du symbole de Legendre (d/p_i) se fait en(voir [Ros]):

$$O\left(\log^2 p_i\right).$$

L'algorithme Ressol (voir Appendice C) peut déterminer une solution de la congruence $t^2 \equiv d \pmod{p_i}$ en:

$$O(\log p_i),$$

en supposant connu un non-résidu quadratique modulo p_i.
Si pour un nombre premier p_i, une solution de la congruence $t^2 \equiv d \pmod{p_i}$ est connue, la congruence $t^2 \equiv d \pmod{p_i^{e_i}}$ peut être résolue par la méthode de Newton en

$$O(e_i \log p_i).$$

Une solution pour chaque congruence $t^2 \equiv d \pmod{p_i^{e_i}}$ peut donc être déterminée en:

$$O\left(\log^2 p_i\right) + O(\log p_i) + O(e_i \log p_i) = O\left(e_i \log^2 p_i\right).$$

Globalement pour les r congruences $t^2 \equiv d \pmod{p_i^{e_i}}$, on a:

$$\sum_{i=1}^{r} O\left(e_i \log^2 p_i\right) = O\left(\log^2 m\right).$$

Le théorème des restes chinois permet alors de déterminer une solution pour la congruence $t^2 \equiv d \pmod m$ en:

$$O\left(\log^2 m\right).$$

Pour chaque solution t, $0 < t < m/2$ de la congruence ci-dessus, il s'agit ensuite de calculer les réduites u_i/v_i de $-t/m$. Ceci se fait en:

$$O(\log m).$$

La vérification des entiers $x_i = tv_i + mu_i$ dans l'équation (10) se fait donc en:

$$O(\log m).$$

Finalement, pour chaque solution de la congruence $t^2 \equiv d \pmod{m}$, la détermination d'une solution pour l'équation (10) se fait en:

$$O\left(\log^2 m\right).$$

Cette complexité ne dépend ni de a ni de b car $0 < a, b < m$. ■

Remarques. 1) En théorie, lorsque m est très grand, sa factorisation peut se faire par exemple suivant la méthode du crible algébrique [L-L-M-P] en:

$$O\left(\exp\left((\log m)^{1/3}(\log\log m)^{2/3}\right)\right).$$

2) La détermination d'un non-résidu quadratique modulo un nombre premier p se fait en (voir [Ha-Mu-Wi]):

$$O\left(p^{(4\sqrt{e})^{-1}+\varepsilon}\right),$$

où $\varepsilon > 0$ est une constante absolue. En pratique un tel non-résidu peut être déterminé souvent rapidement en testant les premiers entiers.

Corollaire 2. *Si la factorisation de m est donnée et si pour chaque nombre premier p divisant m, un non-résidu quadratique modulo p est connu, alors la complexité de l'algorithme* 1 *est:*

$$O\left(2^{\varepsilon \log m/log \log m}\right),$$

où ε est une constante absolue.

Preuve. Chaque solution de la congruence $at^2 + b \equiv 0 \pmod{m}$ peut donner au plus une solution de l'équation $ax^2 + by^2 = m$. La détermination de toutes les solutions de cette équation est donc en:

$$O\left(2^{r+1}\log^2 m\right) = O\left(2^{\varepsilon \log m/log \log m}\right),$$

où ε est une constante absolue. Ceci résulte du fait que le nombre de diviseurs premiers de m est tel que:

$$r + 1 = (1 + o(1)) \log m/\log\log m.$$

Cette complexité ne dépend pas de a et de b. ■

3. L'équation de Pell

a. Résolution de $ax^2 - by^2 = m$

Soient $a > 0$, $b > 0$ et $m \neq 0$ des entiers premiers entre eux deux à deux. Soit (x, y) une solution de l'équation

$$ax^2 - by^2 = m, \tag{12}$$

avec $y > 0$ et $(m, y) = 1$. On suppose que a/b n'est pas un carré parfait.

Définition 1. *Deux solutions* (x, y) *et* (x', y') *de l'équation* (12) *sont associées si et seulement si elles vérifient le système:*

$$\begin{cases} axx' - byy' \equiv 0 \pmod{m}, \\ xy' - yx' \equiv 0 \pmod{m}. \end{cases} \tag{13}$$

Les solutions associées entre elles forment une classe. *La solution fondamentale* d'une classe est la solution (x, y) telle que $|x|$ et y sont minimaux avec en plus $x > 0$ si $(-x, y)$ et (x, y) sont associées, c'est à dire si la classe de solutions est ambigue. On désigne par (α, β) la solution fondamentale de l'équation

$$x^2 - aby^2 = 1. \tag{14}$$

Proposition 3. *Toute solution fondamentale* (x_1, y_1) *d'une classe de solutions de l'équation* (12) *vérifie:*

$$\begin{cases} |x_1| \leq \sqrt{\dfrac{(\alpha+\varepsilon)|m|}{2a}}, \\ y_1 \leq \beta\sqrt{\dfrac{a|m|}{2(\alpha+\varepsilon)}}, \end{cases} \tag{15}$$

avec $\varepsilon =$signe(m).

Preuve. Définissons une nouvelle solution (x_2, y_2) de l'équation (12) par:

$$x_2\sqrt{a} + y_2\sqrt{b} = \left(x_1\sqrt{a} + y_1\sqrt{b}\right)\left(\alpha - \beta\sqrt{ab}\right).$$

Supposons d'abord que $m > 0$, alors:

$$x_2 = \alpha x_1 - \beta b y_1 = \alpha x_1 - \sqrt{\beta^2 ab}\sqrt{y_1^2 b}/\sqrt{a} = \alpha x_1 - \sqrt{\alpha^2 - 1}\sqrt{ax_1^2 - m}/\sqrt{a} > 0.$$

Donc, puisque (x_1, y_1) est la solution fondamentale de sa classe, $x_2 = \alpha x_1 - \beta b y_1 > x_1$ et $x_1(\alpha - 1) \geq \beta b y_1$. D'où

$$x_1^2(\alpha - 1)^2 \geq \beta^2 b^2 y_1^2 = (\alpha^2 - 1)(ax_1^2 - m)/a,$$

ce qui donne la première inégalité de (15).
Supposons maintenant que $m < 0$. Des inégalités $\alpha^2 - ab\beta^2 > 0$ et $by_1^2 - ax_1^2 > 0$, on tire $\alpha^2 y_1^2 > a^2\beta^2 x_1^2$, puis $\alpha y_1 - a\beta x_1 > 0$. D'après la définition de (x_1, y_1), on a:

$$y_2 = \alpha y_1 - a\beta x_1 \geq y_1.$$

Alors

$$(\alpha - 1)^2 b y_1^2 \geq a^2 b \beta^2 x_1^2,$$

d'où l'on tire:

$$(\alpha - 1)^2 (a x_1^2 - m) \geq (\alpha^2 - 1) a x_1^2,$$

puis la première inégalité (15).
Maintenant, la première inégalité de (15) donne:

$$by^2 = ax^2 - m \leq a\frac{(\alpha + \varepsilon)|m|}{2a} - m = \frac{|m|(\alpha - \varepsilon)}{2}.$$

Or $\alpha^2 - \varepsilon^2 = ab\beta^2$. Alors:

$$by^2 \leq \frac{a|m|\beta^2}{2(\alpha + \varepsilon)},$$

ce qui donne la deuxième inégalité de (15). ■

Le théorème suivant lie les solutions de la congruence (5) et les classes de solutions de l'équation (12).

Théorème 4. *Soient $a > 0$, $b > 0$ et m des entiers tels que la congruence* (5) *soit résoluble. Toute classe de solutions de l'équation* (12) *est de la forme*

$$K(t) = \{(x, y) \in \mathbb{Z}^2 | ax^2 - by^2 = m, x \equiv ty \pmod{m}\},$$

où t est une solution de la congruence $t^2 \equiv ba^{-1} \pmod{m}$.

Preuve. Soit K une classe de solutions de (12). Elle admet une solution fondamentale (x_0, y_0). Soit t l'entier vérifiant

$$x_0 \equiv ty_0 \pmod{m}, \quad \text{et} \quad 0 \leq |t| \leq |m|/2.$$

Alors t est une solution de la congruence $t^2 \equiv ba^{-1} \pmod{m}$. Les autres solutions (x, y) de cette classe sont liées à (x_0, y_0) par les relations (13). En les simplifiant, alors $x \equiv ty$ $\pmod{m}$ et donc que $K = K(t)$. ■

Ce théorème montre que le nombre de classes de solutions de l'équation (12) est au plus égal au nombre de solutions de la congruence $t^2 \equiv ba^{-1} \pmod{m}$. Si (x_t, y_t) est la solution fondamentale d'une classe $K(t)$ et (α, β) celle de l'équation (14), alors les autres solutions (x, y) de la classe $K(t)$ sont données par la relation:

$$x\sqrt{a} + y\sqrt{b} = \pm\left(x_t\sqrt{a} + y_t\sqrt{b}\right)\left(\pm\alpha + \beta\sqrt{ab}\right)^n ,$$

où $n \in \mathbb{Z}$.

D'après le théorème 1, on sait résoudre toutes les équations (12) dans lesquelles $ab \geq 4$. Il reste donc à examiner les cas $ab = 2$, $ab = 3$, c'est à dire les cas $(a, b) = (1, 2)$ et $(a, b) = (1, 3)$. On va montrer maintenant que ces cas ne sont à étudier que lorsque $m < 0$. Dans les deux cas qui suivent, on a $a = 1$ et $b = 2, 3$.

(a) Supposons que $m > 0$. Alors toute solution (x, y) de (12) est telle que $x^2 - by^2 = m > 0$ et donc:

$$\frac{|x|}{y} > \sqrt{b}.$$

D'autre part, toute solution de (12) est déterminée par $x = tv - mu \neq 0$ et $y = v$, où t vérifie $x \equiv ty \pmod{m}$ avec $0 \leq |t| \leq m/2$, alors, en désignant par δ le signe de x et en utilisant la relation:

$$\left|\frac{x}{y} + \delta\sqrt{b}\right| = \frac{|x|}{y} + \sqrt{b} > 2\sqrt{b} > 2,$$

on a:

$$\left|\frac{x}{y} - \delta\sqrt{b}\right| = \frac{m}{\left|x/y + \delta\sqrt{b}\right| y^2} < \frac{m}{2y^2},$$

ce qui implique:

$$\left|\frac{t - \delta\sqrt{b}}{m} - \frac{u}{v}\right| < \frac{1}{2v^2}.$$

Il en résulte alors que $\frac{u}{v}$ est une réduite de $\frac{t - \delta\sqrt{b}}{m}$.

(b) Si $m < 0$ et $b = 2$ (avec $a = 1$), alors toute solution (x, y) de (12) est déterminée par le produit:

$$x + y\sqrt{2} = (U + V\sqrt{2})(\pm 1 + \sqrt{2})^{2n+1}$$

où $n \in \mathbb{Z}$ et où (U, V) est une solution de l'équation:

$$U^2 - 2V^2 = -m$$

qui peut être résolue par la méthode précédente puisque $-m > 0$.

Si $m < 0$ et $b = 3$, alors en multipliant (12) par -3 et en posant $V = x$ et $U = 3y$, on obtient l'équation équivalente:

$$U^2 - 3V^2 = -3m$$

où $-3m > 0$ et qui peut donc être résolue par la méthode décrite au (a).

Dans la partie 4 qui suit, on va écrire un algorithme pour résoudre les équations de Pell avec $ab \geq 4$. Cet algorithme est basé sur le calcul des réduites u/v de nombres réels $\left(t \pm \sqrt{b/a}\right)/m$, puis de $-\left(t \pm \sqrt{ba}\right)/m$ pour le second algorithme, pour chaque solution t, $0 \leq t \leq |m|/2$ de la congruence $t^2 \equiv ba^{-1} \pmod{m}$. On peut économiser les calculs en utilisant le lemme suivant:

Lemme 3. *Soit ξ un nombre réel. On pose $\nu = \xi - [\xi]$. Alors:*
i) *Si $\nu \leq 1/2$, alors toute réduite de ξ est l'opposée d'une réduite de $-\xi$.*
ii) *Si $\nu > 1/2$ alors toute réduite de $-\xi$ est l'opposée d'une réduite de ξ.*

Preuve. Développons ξ en fraction continue, $\xi = [a_0, a_1, a_2, \ldots]$. On a $a_0 = [\xi]$ et $a_1 = [1/\nu]$. Pour démontrer (i), supposons que $\nu \leq 1/2$. Alors $a_1 \geq 2$ et

$$-\xi = [-a_0 - 1, 1, a_1 - 1, a_2, a_3, \ldots].$$

Soient u_i/v_i et u_i'/v_i', $i = -2, -1, \ldots$ les réduites de ξ et $-\xi$ respectivement. Alors il est simple de montrer que pour tout $i \geq 1$, $u_i' = -u_{i-1}$ et $v_i' = v_{i-1}$.
Pour démontrer (ii), il suffit de remarquer si $\xi - [\xi] > 1/2$, alors $-\xi - [-\xi] \leq 1/2$. On peut donc appliquer (i) en remplaçant ξ par $-\xi$. ■

Il existe d'autres algorithmes pour résoudre les équations de Pell, en particulier, celui qui est décrit dans [Fai] utilise des notions algébriques plus générales que celles utilisées dans notre version.

b. Algorithme 2. ($ax^2 - by^2 = m$)

L'algorithme qu'on va écrire maintenant suppose qu'on a l'une ou l'autre des conditions (a) ou (b) suivantes:
(a) $m > 0$,
(b) $m < 0$ et $ab \geq 4$.
Comme on l'a vu précédemment, les cas $(a, b) = (1, 2)$ ou $(a, b) = (1, 3)$ peuvent toujours se remener au cas (a) ou au cas (b).

Entrée: $a > 0$, $b \neq 0$, $m = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$;

La solution fondamentale (α, β) de l'équation $x^2 - aby^2 = 1$;

Initialisation: Déterminer les solutions t_j, $j = 1, \cdots, n_0$ de $t^2 \equiv ba^{-1} \pmod m$ telles que $0 < |t_j| < m/2$;

s :=signe(m);
$j := 0$;
Tant que $j \leq n_0 - 1$ **répéter**
  $j := j + 1$;
  $h := 0$;
  Tant que $h \leq 1$ **répéter**
    $h := h + 1$;
    Si $h = 1$ **alors** $\varepsilon := -1$ **sinon** $\varepsilon := 1$;
    $\xi_{j,h} := (t_j + \varepsilon\sqrt{b/a})/m$.
    Si $\xi_{j,h} - [\xi_{j,h}] > 1/2$ **faire**
      $i := 0$;
      $y_0 := 1$;
      $q := 0$;
      Tant que $y_i < \beta\sqrt{a|m|/2(\alpha + s)}$ **et** $q \neq 1$ **répéter**
        $x_i := t_j y_i - m u_i$;
        Si $|x_i| < \sqrt{(\alpha + s)|m|/2a}$ **faire**
          $q := (ax_i^2 - by_i^2)/m$;
          Si $q = 1$ écrire x_i et y_i;
        $i := i + 1$;
        Calculer la réduite u_i/y_i de $\xi_{j,h}$;

Sortie: Les solutions fondamentales (x, y) telles que $ax^2 - by^2 = m$. ■

c. Complexité de l' algorithme 2

Dans cette partie, nous déterminons la complexité de l'algorithme 2.

Théorème 5. *Si la factorisation de m et la solution fondamentale de l'équation $x^2 - aby^2 = 1$ sont données, alors la détermination d'une solution fondamentale pour l'équation $ax^2 - by^2 = m$ se fait en:*

$$O\left(\sqrt{ab}\log ab|m|\right).$$

Preuve. Une partie de la complexité de l'algorithme 2 a été étudiée dans la preuve du théorème 3. Nous supposons ici que la factorisation de m et la solution fondamentale de l'équation $x^2 - aby^2 = 1$ sont données. En théorie, la solution fondamentale peut être déterminer en:

$$O\left(\sqrt{ab}\log ab\right),$$

(voir [Hua]), ce qui permet d'avoir la majoration suivante:

$$\max(\alpha, \beta) \leq c_0^{\sqrt{ab}\log ab},$$

où c_0 est une constante absolue. Une solution de la congruence $t^2 \equiv ba^{-1}$ est déterminée (voir démonstration du théorème 3) en:

$$O\left(\log^2 m\right).$$

Pour une solution t, il s'agit ensuite de calculer des réduites u_i/y_i de deux nombres réels liés à t en se limitant aux réduites u_i/v_i vérifiant

$$y_i < \beta\sqrt{a|m|/2(\alpha \pm 1)} \leq |m| c_0^{\sqrt{ab}\log ab}.$$

Ces réduites peuvent être calculées en:

$$O\left(\log|m| + \sqrt{ab}\log ab\right) = O\left(\sqrt{ab}\log(ab|m|)\right).$$

Ensuite, pour la même solution t, il s'agit de tester les entiers $x_i = tu_i - my_i$ et y_i dans l'équation $ax^2 - by^2 = m$. Ceci se fait en:

$$O\left(\sqrt{ab}\log(ab|m|)\right).$$

Ceci termine la preuve du théorème. ■

Corollaire 3. *La complexité de l'algorithme 2 est:*

$$O\left(2^{\varepsilon \log|m|/\log\log|m|}\sqrt{ab}\log ab\right),$$

où $\varepsilon > 0$ est une constante absolue.

Preuve. Si la congruence $t^2 \equiv ba^{-1} \pmod{m}$ admet 2^{r+2} solutions, alors la complexité totale de l'algorithme 2 est en:

$$O\left(\log^2|m|\right) + O\left(2^{r+1}\sqrt{ab}\log ab|m|\right) = O\left(2^{\varepsilon \log|m|/\log\log|m|}\sqrt{ab}\log ab\right),$$

où ε est une constante absolue. ■

III. Applications des équations de Thue

1. Le quotient de Szpiro pour quelques familles de courbes elliptiques

Rappelons que pour une courbe elliptique E définie sur $\mathbb{Q}$, semi-stable, de discriminant minimal Δ_E et de conducteur $N_E = r(\Delta_E)$, le quotient de Szpiro est:

$$\sigma_E = \frac{\log|\Delta_E|}{\log N_E}.$$

Soient a et b deux entiers premiers entre eux tels que $ab(a-b) \neq 0$. On définit une courbe elliptique E par le modèle de Wierstrass suivant:

$$E : y^2 + (b^2 + ab - a^2)xy + a^2b^3(b-a)y = x^3 + a^2b(b-a)x^2.$$

Ses invariants $c_4(a,b)$ et $\Delta(a,b)$ sont:

$$\begin{aligned} c_4(a,b) &= (a^2 - ab + b^2)(a^6 - 11a^5b + 30a^4b^2 - 15a^3b^3 - 10a^2b^4 + 5ab^5 + b^6), \\ \Delta(a,b) &= a^7b^7(a-b)^7(a^3 - 8a^2b + 5ab^2 + b^3). \end{aligned}$$

Remarque. L'équation de E paramètre les courbes elliptiques qui ont un point rationnel d'ordre 7.

La proposition suivante précise la minimalité du modèle ci-dessus est la semi-stabilité de la courbe elliptique E:

Proposition 3. *Soient a et b deux entiers premiers entre eux tels que $ab(a-b) \neq 0$. Soit $g = (\Delta(a,b), c_4(a,b))$. Alors $g = (a^2 - ab + b^2, a^3 - 8a^2b + 5ab^2 + b^3)$ et $g = 1$ ou $g \equiv 0 \pmod{49}$. En particulier, lorsque $g = 1$, la courbe elliptique E est semi-stable et son modèle est minimal.*

Preuve. Soit p un diviseur premier de $\Delta(a,b)$.
- Si $p|a$, alors p ne divise pas b et donc p ne divise pas $c_4(a,b)$.
- Si $p|b$, on a la même conclusion.
- Si $p|(a-b)$, alors en posant d=a-b, on peut écrire:

$$c_4(a,b) = \left(d^2 + ab\right)(d^6 - 5bd^5 - 10b^2d^4 + 15b^3d^3 + 30b^4d^2 + 11b^5d + b^6),$$

et donc p ne divise pas $c_4(a,b)$.
- Si $p|a^3 - 8a^2b + 5ab^2 + b^3$, alors p ne divise ni a, ni b.

Supposons que $p|a^2 - ab + b^2$. En utilisant l'égalité:

$$a^3 - 8a^2b + 5ab^2 + b^3 = (a - 7b)(a^2 - ab + b^2) - b^2(3a - 8b),$$

alors $p|3a - 8b$. En utilisant l'égalité:

$$9(a^2 - ab + b^2) = (3a + 5b)(3a - 8b) + 49b^2,$$

alors $p|49b^2$ et donc $p = 7$.
Supposons que $p|a^6 - 11a^5b + 30a^4b^2 - 15a^3b^3 - 10a^2b^4 + 5ab^5 + b^6$. En utilisant l'égalité:

$$\begin{aligned} &a^6 - 11a^5b + 30a^4b^2 - 15a^3b^3 - 10a^2b^4 + 5ab^5 + b^6 \\ &= (a^3 - 8a^2b + 5ab^2 + b^3)^2 + b(a^3 - 8a^2b + 5ab^2 + b^3) + b^4(44a^2 - 31ab - 6b^2), \end{aligned}$$

alors $p|44a^2 - 31ab - 6b^2$. Maintenant en utilisant l'égalité:

$$1936(a^3 - 8a^2b + 5ab^2 + b^3) = (44a^2 - 31ab - 6b^2)(44a - 321b) - b^2(7a - 10b),$$

alors $p|7a - 10b$. En utilisant l'égalité:

$$49(44a^2 - 31ab - 6b^2) = (7a - 10b)(308a + 223b) + 1936b^2,$$

alors p divise $1936 = 2^4.11^2$. Alors $p = 2$ ou $p = 11$, ce qui est impossible car dans ce cas $p|a^3 - 8a^2b + 5ab^2 + b^3$ mais la congruence

$$t^3 - 8t^2 + 5t + 1 \equiv 0 \pmod p,$$

n'a pas de solution.
Nous venons de montrer que $(\Delta(a, b), c_4(a, b)) = (a^2 - ab + b^2, a^3 - 8a^2b + 5ab^2 + b^3)$ et que si 7 ne divise pas ce pgcd, alors ces deux invariants sont premiers entre eux. Ceci implique alors dans ce cas que le modèle de la courbe elliptique E est minimal et qu'elle est semi-stable (voir Appendice A). ■

Nous allons considérer une courbe 7-isogène de la courbe elliptique E. Soient a et b deux entiers premiers entre eux tels que $ab(a - b) \neq 0$. On définit une nouvelle courbe elliptique E' par le modèle de Wierstrass suivant:

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$

avec:
$a_1 = b^2 + ab - a^2$,

$a_2 = a^2b(b-a),$
$a_3 = a^2b^3(b-a),$
$a_4 = 5ab(b-a)(a^2-ab+b^2)(a^3+2a^2b-5ab^2+b^3),$
$a_6 = ab(b-a)(a^9+9a^8b-37a^7b^2+70a^6b^3-132a^5b^4+211a^4b^5-182a^3b^6+76a^2b^7-18ab^8+b^9).$

Ses invariants $c_4'(a,b)$ et $\Delta'(a,b)$ sont:

$$c_4'(a,b) = (a^2-ab+b^2)(a^6+229a^5b+270a^4b^2-1695a^3b^3+1430a^2b^4-235ab^5+b^6),$$
$$\Delta'(a,b) = ab(a-b)(a^3-8a^2b+5ab^2+b^3)^7.$$

La proposition 3 précise aussi la minimalité du modèle ci-dessus et la semi-stabilité de la courbe elliptique E'. La preuve reste identique, à quelques changements près. En particulier, si $(\Delta'(a,b), c_4'(a,b)) = 1$, alors le modèle ci-dessus est minimal et la courbe elliptique E' est semi-stable. ■

Nous remarquons que la même expression $a^3-8a^2b+5ab^2+b^3$ figure dans les discriminants des deux courbes elliptiques E et E'. Nous pouvons donc chercher des valeurs de a et de b de telle sorte que cette expression soit assez grande par rapport à son radical.
Soit m un entier strictement positif. On considère alors l'équation:

$$x^3-8x^2y+5xy^2+y^3 = mz, \tag{16}$$

en entiers $x \neq 0$, $y > 0$, $z \neq 0$ et tels que $(y,m) = 1$ et z petit. Nous lui appliquerons alors la méthode décrite dans la partie I de ce même chapitre.
L'équation

$$\theta^3-8\theta^2+5\theta+1 = 0,$$

admet trois racines réelles:

$$\theta_1 = (8-14\sin(\omega))/3,$$
$$\theta_2 = \left(8+7\sqrt{3}\cos(\omega)+7\sin(\omega)\right)/3,$$
$$\theta_3 = \left(8-7\sqrt{3}\cos(\omega)+7\sin(\omega)\right)/3,$$

avec

$$\omega = \frac{1}{3}\arctan\left(\frac{13\sqrt{3}}{9}\right).$$

On considère ensuite la congruence:

$$t^3-8t^2+5t+1 \equiv 0 \pmod{m}. \tag{17}$$

Soient t_i, $1 \leq i \leq r$ ses différentes solutions avec $0 \leq |t_i| \leq m/2$. Le théorème 1 permet de trouver des solutions de l'équation (16) en prenant $x = t_i v - mu$ et $y = v$ où u et v sont deux entiers tels que u/v est une réduite de $\dfrac{t_i - \theta_j}{m}$, pour $1 \leq i \leq r$ et $j = 1, 2, 3$. Ces réduites doivent vérifier $v > V_1(\theta_j)$ avec

$$V_1(\theta_1) \simeq 1.217, \qquad V_1(\theta_2) \simeq 1.050, \qquad V_1(\theta_3) \simeq 0.167.$$

Nous allons maintenant étudier la congruence (17). Ecrivons d'abord m sous forme de produits de facteurs premiers $m = 2^e p_1^{e_1} \dots p_r^{e_r}$. La congruence (17) est équivalente au système:

$$\begin{cases} t^3 - 8t^2 + 5t + 1 \equiv 0 \pmod{2^e}, \\ t^3 - 8t^2 + 5t + 1 \equiv 0 \pmod{p_i^{e_i}} \quad 1 \leq i \leq r. \end{cases}$$

La congruence modulo 2^e est impossible, donc m doit être impair. Les congruences modulo $p_i^{e_i}$ ne sont résolubles que pour certaines valeurs de p_i . Nous supposons donc que m est composé de nombres premiers pour lesquels la congruence est résoluble et que $p_i \neq 7$ pour tout i. Nous considérons donc la congruence:

$$t^3 - 8t^2 + 5t + 1 \equiv 0 \pmod{p^e}, \tag{18}$$

avec $0 < t < p^e$. Soit t_1 une solution de cette congruence avec $e = 1$. Le lemme de Hensel permet de trouver une solution de la congruence (18), en utilisant les formules de récurrence:

$$\begin{cases} a_1 = t_1, \\ t_{k+1} \equiv t_k - (3t_k^2 - 16t_k + 5)^{-1}(t_k^3 - 8t^2 + 5t + 1) \pmod{p^{k+1}}, \end{cases}$$

pour tout k, $1 \leq k \leq e - 1$, avec $0 < t_{k+1} < p^{k+1}$ et un inverse $(3t_k^2 - 16t_k + 5)^{-1}$ pris modulo p. L'existence de $(3t_k^2 - 16t_k + 5)^{-1} \pmod{p}$ est assurée par la proposition suivante:

proposition 4. *Soit p un nombre premier impair et différent de 7. Le système:*

$$\begin{cases} t^3 - 8t^2 + 5t + 1 \equiv 0 \pmod{p}, \\ 3t^2 - 16t + 5 \equiv 0 \pmod{p}, \end{cases}$$

n'a pas de solution.

Preuve. Toute solution du système de cette proposition vérifie la congruence:

$$8t^2 - 10t - 3 \equiv 0 \pmod{p},$$

dont les solutions sont $t_1 = 3(p^2+1)/2$ et $t_2 = (p^2-1)/4$. En remplaçant t par t_1 dans la deuxième équation du système, on obtient:

$$27p^2 - 22p - 49 \equiv 0 \pmod{p},$$

qui est impossible puisque $p \neq 7$. En remplaçant t par t_2 dans la première équation du système, on obtient:

$$p^6 - 35p^4 + 147p^2 - 49 \equiv 0 \pmod{p},$$

qui est impossible aussi. ■

Le théorème des restes chinois permet ensuite de déterminer toutes les solutions de la congruence (17).

En application numérique, nous avons pris des entiers positifs $m = p^e$ avec $1 \leq p \leq 10000$ et $1 \leq e \leq 100$ et nous avons ainsi déterminé des solutions (x, y) de l'équation

$$x^3 - 8x^2y + 5xy^2 + y^3 = mz,$$

vérifiant $(x, y) = 1$, $y > 0$ et tels que 7 ne divise pas mz et $|z|$ petit. Nous avons alors calculé les quotients:

$$\sigma_E = \frac{\log |a|^7 b^7 |a-b|^7 |a^3 - 8a^2b + 5ab^2 + b^3|}{\log r\left(ab(a-b)(a^3 - 8a^2b + 5ab^2 + b^3)\right)},$$

$$\sigma_{E'} = \frac{\log |a||b||a-b||a^3 - 8a^2b + 5ab^2 + b^3|^7}{\log r\left(ab(a-b)(a^3 - 8a^2b + 5ab^2 + b^3)\right)},$$

correspondant aux quotients de Szpiro des courbes elliptiques E et E' définies par les équations du début de cette partie. Nous avons résumé dans les tables 1 et 2 les plus grandes valeurs de σ_E et $\sigma_{E'}$ qui sont supérieur à 6.50 et 7.00 respectivement. Ces quotients sont assez éloignés de la valeur conjecturale 6, donnée dans la conjecture de Szpiro forme forte (voir chapitre 1, partie I).

Certains exemples ont été déterminer partir des bonnes relations abc des tables figurant à la fin du chapitre 4. Ces exemples sont signalés par un astérisque $*$ dans la colonnes de p.

Table 1

p	a	b	a - b	a^3-$8a^2b$+$5ab^2$+b^3	σ_E
587	$2^{15}.13$	$31^2.59$	3.5.7.3517	$587^4.17011$	7.36246
2659	$2^6.7^2.47$	$3^5.83$	29.41.107	251.2659^3	7.10618
$*$	$2^{11}.7^4.9049$	19^8	31^7	$-937^2.\cdots$	6.80043
197	384079	$3^2.5.37.79$	$2^7.1973$	$-13.83.197^6$	6.76452
9533	$2^6.7.37.83$	3^{13}	$-5.11.29.137$	$-71.9533^2.21323$	6.69128
13	149.1423	$5^2.43.113$	$2^3.3.7^3.11$	$-13^{10}.121283$	6.66500
13	2	11	-9	13^3	6.61959
127	$-2^5.17$	$5^2.137$	$-3^4.7^2$	127.3583	6.58656
337	$2^2.499.1033.500287$	$3^2.5^8.139.2447$	$\cdots$	$337^9.\cdots$	6.53638
251	$2^5.71^3$	$3^3.53.1097$	5.29.68161	$13.251^3.617.1777$	6.51985
181	11.17^2	3.5.29	$2^3.7^3$	$13.113.181^2$	6.50949

Les pointillés ($\cdots$) remplacent des produits de facteurs premiers avec un exposant égal à 1.

Table 2

p	a	b	a - b	$a^3 - 8a^2b + 5ab^2 + b^3$	$\sigma_{E'}$
13	2	11	-3^2	13^3	8.75732
41	-2.3^5	1	-487	$-41^3.1693$	7.44460
41	-283	3.7	$-2^4.19$	-13.41^4	7.32780
$*$	5^4	$2^5.17$	3^4	$-83^2.53719$	7.20525
113	$17^2.229$	29^2	$2^2.3^3.5.11^2$	$13.113^4.122963$	7.16913
587	$2^15.13$	$31^2.59$	3.5.7.3517	$587^4.17011$	7.13801
419	$-2^3.3^3.13$	7	-5.563	-307.419^3	7.10156

2. Les nombres de Ramanujan

Définition 2. *Un entier $m > 0$ est appelé nombre de Ramanujan s'il s'écrit de deux façons différentes sous forme de somme de deux cubes positifs premiers entre eux.*

Un exemple célèbre est le nombre 1729, découvert par Ramanujan lui même:

$$1729 = 9^3 + 10^3 = 1^3 + 12^3.$$

C'est aussi le plus petit nombre de Ramanujan.
Dans cette partie, nous allons montrer comment en trouver d'autres. Nous allons commencer par étudier l'équation de Thue:

$$x^3 + y^3 = m, \tag{19}$$

en entiers x et y vérifiant $0 < y < x < m^{1/3}$ et $(m, y) = 1$ où m est donné. On va commencer par démontrer la proposition suivante qui nous permettra de ne pas envisager les cas $m = p^e$ où p est un nombre premier.

Proposition 5. *Si $m = p^e$ avec p premier et e entier positif, alors l'équation (19) n'admet pas de solution vérifiant $(y, m) = 1$, $0 < y < x$ sauf dans le cas $m = 3^2$ et alors $1^3+2^3 = 3^2$.*

Preuve. Soit $m = p^e$ avec p premier et $e \geq 1$. La factorisation

$$(x + y)(x^2 - xy + y^2) = p^e,$$

implique que x et y vérifient le sytème:

$$\begin{cases} x + y = p^i, \\ x^2 - xy + y^2 = p^j, \\ 0 \leq i, j, \quad i + j = e. \end{cases}$$

Le cas $i = 0$ ne peut pas avoir lieu, sinon $y = 0$. Le cas $j = 0$ ne peut pas avoir lieu non plus, sinon on aurait:

$$x^2 - xy + y^2 = (x - y)^2 + xy = 1,$$

et donc $y = 0$. Maintenant on a $i \geq 1$ et $j \geq 1$ dans le système ci-dessus. De l'égalité $x^2 - xy + y^2 = (x + y)^2 - 3xy$, il résulte que $3xy = p^{2i} - p^j > 0$ et donc que $2i > j$ et que $p^j|3xy$. Si $p|x$ (resp. $p|y$), alors $p|y$ (resp. $p|x$). Il reste donc le cas $p^j|3$ et donc $p = 3$ et $j = 1$. La deuxième équation de ce système devient alors:

$$x^2 - xy + y^2 = (x - y)^2 + xy = 3,$$

et donc $y = 1$ et $x = 2$. ■

Nous allons décrire deux méthodes pour résoudre l'équation (19).

(a). Première méthode. Nous allons utiliser la méthode de résolution des équations de Thue basée sur les fractions continues. On commence par édutier la congruence:

$$t^3 + 1 \equiv 0 \pmod{m}, \tag{20}$$

avec $0 < t < m$. Ecrivons m sous la forme $m = p_1^{e_1} \cdots p_r^{e_r}$, où chaque p_i, $1 \leq i \leq r$ est un nombre premier et où chaque exposant e_i, $1 \leq i \leq r$ est strictement positif. La congruence ci-dessus se décompose en r congruences:

$$t^3 + 1 \equiv 0 \pmod{p^e}. \tag{21}$$

Le nombre de solutions de cette congruence est égal à $(3, p^{e-1}(p-1)$. On distingue alors les cas suivants:
- Si $p = 3$ alors cette congruence admet une solution t =2 si $e = 1$ ou trois solutions $t = 3^{e-1} - 1, 2 \times 3^{e-1} - 1, 3^e - 1$, si $e \geq 2$.
- Si $p \not\equiv 1 \pmod 3$, la congruence (21) admet la seule solution $t = p^e - 1$.
- Si $p \equiv 1 \pmod 3$, la congruence (21) admet trois solutions $t = p^e - 1, t_0, t_0^{-1}$ avec $0 < t_0 < p^e$ et t_0^{-1} est pris modulo p^e. Pour déterminer la solution t_0, on commence par détérminer une solution $s_1 \neq p - 1$ de la congruence (21) avec $e = 1$, puis on utilise les relations de récurrence:

$$s_{i+1} \equiv s_i - (3s_i)^{-1}(s_i^3 + 1) \equiv p^{i+1},\ 1 \leq i \leq e - 1,$$

où $(3s_i)^{-1}$ est pris modulo p et où s_i est tel que $0 < s_i < p^i$. Une solution de la congruence (21) est alors $t_0 = s_e$. En remarquant que $s_e \equiv s_1 \not\equiv -1 \pmod p$, alors $t_0 \neq p^e - 1$.

Cette première méthode utilise le dévelopement du rationnel t/m en fraction continue, où t est une solution de la congruence (20). Si cette congruence n'admet qu'une seule solution, c'est précisement $t = m - 1$ et le développement de $\dfrac{m-1}{m}$ en fraction continue est:

$$\frac{m-1}{m} = [0, 1, m-1].$$

Les réduites de ce développement sont $u_0/v_0 = 0/1$, $u_1/v_1 = 1/1$ et $u_2/v_2 = (m-1)/m$. En remplaçant dans les égalités:

$$(tv_i - mu_i)^3 + v_i^3 = mz_i, \quad 0 \leq i \leq 2,$$

on obtient successivement:
(i) $(m-1)^3+1^3=m(m^2-3m+3)$, mais $m^2-3m+3\neq 1$ pour $m\geq 1729$,
(ii) $(-1)^3+1^3=0$, ce qui n'a pas d'interêt,
(iii) $0^3+m^3=m^3$, ce qui non plus n'a pas d'interêt.
Ainsi, lorsque la congruence (20) n'a qu'une solution, on peut ne pas traiter l'équation (19), qui de toute façon n'admet pas deux solutions distinctes. ■

Il arrive toutefois que le nombre de solutions de la congruence (20) soit assez grand et dans ce cas le nombre de réels à développer en fraction continue est aussi assez grand. La méthode décrite ci-dessus devient alors impraticable. Il est préférable d'utiliser la deuxième méthode.

(b). Deuxième méthode. Toute solution de l'équation (19) vérifie:

$$x^3+y^3=(x+y)(x^2-xy+y^2)=m.$$

Il suffit donc de prendre

$$\begin{cases} x+y=a, \\ x^2-xy+y^2=b, \end{cases}$$

où a et b sont tels que $ab=m$. D'après l'égalité:

$$x^2-xy+y^2=(x+y)^2-3y(x+y)+3y^2,$$

on a:

$$(x+y,x^2-xy+y^2)|3.$$

On écrit donc m de deux façons suivant que $9|m$ ou non. Si $9|m$, on écrit $m=3^{e-1}.3.p_1^{e_1}\cdots p_r^{e_r}$ avec $e\geq 2$, sinon, on écrit $m=3^e p_1^{e_1}\cdots p_r^{e_r}$, avec $e\leq 1$ et où les p_i, $1\leq i\leq r$ sont des nombres premiers différents de 3. On peut finalement écrire $m=d_1d_2\cdots d_k$. Alors la factorisation ab de m doit être telle que $(a,b)|3$. Il y a donc 2^k possibilités pour choisir un couple (a,b) avec cette propriété. Une fois a et b choisis, toute solution (x,y) vérifie le système:

$$\begin{cases} x^2-xy+y^2=b, \\ y=a-x. \end{cases}$$

Alors x est donné par:

$$x=\frac{3a\pm\sqrt{12b-3a^2}}{6}.$$

Alors a et b doivent être choisis pour que les racines ci-dessus soient entières, ce qui donne un test pour les couples (a,b). ■

Nous disposons maintenant de tous les moyens pour chercher des nombres de Ramanujan. Etant donné un entier $m > 0$, qui n'est pas de la forme $m = p^e$ où p est un nombre premier, et qui est tel que la congruence (20) ait au moins trois solutions, on peut résoudre l'équation (19) en prenant $x = tv - mu$ et $y = v$ où u/v est une réduite de t/m où t est une solution de la congruence (20). Si toutefois le nombre de solutions de la congruence (20) est plus grand que le nombre de couples (a, b) tels que $m = ab$ et $(a, b)|3$, nous utilisons plutôt la deuxième méthode.

Nous avons ainsi testé tous les entiers $m < 2.10^8$. Il y a exactement 99 entiers parmi eux ayant deux représentations positives de la forme $x^3 + y^3 = m$ avec $0 < x < y$ et $(y, m) = 1$. Nous avons listé ces représentations pour les entiers $m < 10^7$ dans la table 3.

Dans la table 4 ci-dessous, nous avons dressé aussi la liste des entiers $m < 10^7$ qui ont trois représentations de la forme $x^3 + y^3 = m$ avec pour seule condition $(x, y) = 1$. Il y a en fait 55 entiers $m < 2.10^8$ qui ont trois de telles représentations.

Dans leur livre, J. Silverman et J. Tate ([Sil-Tat], p. 151) affirment que le plus petit entier pouvant s'écrire de trois façons différentes est:

$$3242197 = 76^3 + 141^3 = 85^3 + 138^3 = -171^3 + 202^3.$$

La table 4 montre que ceci est faux. J. H. Silverman se trompe aussi sur le plus petit entier sans facteurs cubiques admettant trois représentations (voir [Sil3]). Ce nombre est présisement le premier exemple de la table 4. Le même auteur ne connaissait pas d'entiers sans facteurs cubiques admettant quatre représentations. Nous avons pu le déterminer:

$$16776487 = -201^3 + 292^3 = -9^3 + 256^3 = 183^3 + 220^3 = 58^3 + 255^3.$$

Table 3

m	$x_1^3 + y_1^3$	$x_2^3 + y_2^3$
1729	$1^3 + 12^3$	$9^3 + 10^3$
20683	$10^3 + 27^3$	$19^3 + 24^3$
40033	$16^3 + 33^3$	$9^3 + 34^3$
149389	$8^3 + 53^3$	$29^3 + 50^3$
195841	$9^3 + 58^3$	$22^3 + 57^3$
327763	$30^3 + 67^3$	$51^3 + 58^3$
443889	$17^3 + 76^3$	$38^3 + 73^3$
684019	$51^3 + 82^3$	$64^3 + 75^3$
704977	$2^3 + 89^3$	$41^3 + 86^3$
1845649	$49^3 + 120^3$	$42^3 + 121^3$
2048391	$2^3 + 127^3$	$95^3 + 106^3$
3242197	$76^3 + 141^3$	$85^3 + 138^3$
3375001	$73^3 + 144^3$	$1^3 + 150^3$
4342914	$23^3 + 163^3$	$121^3 + 137^3$
4931101	$102^3 + 157^3$	$76^3 + 165^3$
5772403	$51^3 + 178^3$	$115^3 + 162^3$
5799339	$107^3 + 166^3$	$40^3 + 179^3$
6058747	$99^3 + 172^3$	$120^3 + 163^3$
7620661	$45^3 + 196^3$	$133^3 + 174^3$
8872487	$14^3 + 207^3$	$140^3 + 183^3$
9443761	$68^3 + 209^3$	$146^3 + 185^3$

Table 4

m	$x_1^3 + y_1^3$	$x_2^3 + y_2^3$	$x_3^3 + y_3^3$
3367	$-33^3 + 34^3$	$-9^3 + 16^3$	$-2^3 + 15^3$
68913	$-86^3 + 89^3$	$-2^3 + 41^3$	$17^3 + 40^3$
152551	$-225^3 + 226^3$	$-24^3 + 55^3$	$-17^3 + 54^3$
195841	$-225^3 + 256^3$	$9^3 + 58^3$	$22^3 + 57^3$
625177	$-456^3 + 457^3$	$-66^3 + 97^3$	$-47^3 + 90^3$
684019	$-477^3 + 478^3$	$51^3 + 82^3$	$64^3 + 75^3$
1147627	$-618^3 + 619^3$	$-165^3 + 178^3$	$-72^3 + 115^3$
1548729	$-95^3 + 134^3$	$-23^3 + 116^3$	$86^3 + 97^3$
2628073	$-135^3 + 172^3$	$-71^3 + 144^3$	$1^3 + 138^3$
2985983	$-73^3 + 150^3$	$-1^3 + 144^3$	$71^3 + 138^3$
3242197	$-171^3 + 202^3$	$76^3 + 141^3$	$85^3 + 138^3$
3442887	$-617^3 + 620^3$	$-4^3 + 151^3$	$-41^3 + 152^3$
4488211	$-80^3 + 171^3$	$-204^3 + 235^3$	$54^3 + 163^3$
4663295	$-193^3 + 228^3$	$-121^3 + 186^3$	$18^3 + 167^3$
4931101	$-192^3 + 229^3$	$102^3 + 157^3$	$76^3 + 165^3$
5318677	$-1331^3 + 1332^3$	$37^3 + 174^3$	$136^3 + 141^3$
7194889	$-423^3 + 436^3$	$-167^3 + 228^3$	$18^3 + 193^3$
8741691	$-197^3 + 254^3$	$-5^3 + 206^3$	$163^3 + 164^3$
9429245	$-1773^3 + 1774^3$	$-282^3 + 317^3$	$162^3 + 173^3$
9667693	$-675^3 + 682^3$	$-51^3 + 214^3$	$16^3 + 213^3$

CHAPITRE 3

Algorithms for finding good abc-examples

I. Introduction

II. On a diophantine equation

III. The algorithm

IV. Relation between t and c-t when n is even

V. Application to special values of c

Algorithms for finding good *abc*-examples

Let $n \neq 0$ be an integer and let $r(n)$ be the radical of n, i.e. the product of the primes dividing n. The abc-conjecture and the Szpiro conjecture imply that for any positive relatively prime integers a, b, and c such that $a + b = c$, the expressions

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

and

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

are bounded. More precisely, the Szpiro conjecture says that for any semi-stable elliptic curve over $\mathbb{Q}$ with discriminant Δ and conductor N, the ratio

$$\sigma = \frac{\log |\Delta|}{\log N}$$

is bounded. We give an algorithm for finding good abc-examples relatively to α and ρ. This algorithm is based on approximation methods for solving the equation $ax^n - by^n = cz$ in integers x, y, and z with small $|z|$.

I. Introduction

An abc-example is a triplet of positive relatively prime integers a, b and c such that $a + b = c$ with $a < b < c$. Define the radical G of abc as the product of all distinct primes dividing abc. The abc-conjecture of Masser and Oesterlé implies that the expression

$$\alpha = \alpha(a, b, c) = \frac{\log c}{\log G} \tag{1.1}$$

is bounded (see [Oesterlé 1988]). The conjectured asymptotic value of $\alpha(a, b, c)$ is 1, so we will say that an abc-example is good relatively to the abc-conjecture if $\alpha(a, b, c) \geq 1.4$.

Let E be a semi-stable elliptic curve over $\mathbb{Q}$ with minimal discriminant Δ and conductor N. The original Szpiro conjecture says that for a given $\varepsilon > 0$, there exists $c(\varepsilon)$ such that

$$|\Delta| \leq c(\varepsilon) N^{6+\varepsilon} \ .$$

This inequality implies that the Szpiro ratio

$$\sigma = \frac{\log |\Delta|}{\log N} \tag{1.2}$$

is bounded. If we apply this conjecture to the elliptic curve

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

where $a \equiv -1 \pmod 4$, $b \equiv 0 \pmod{16}$, $(a,b) = 1$ and $a + b = c$, we get that the expression

$$\rho = \rho(a,b,c) = \frac{\log |abc|}{\log G} \tag{1.3}$$

is bounded ([Oesterlé 1988]). The conjectured asymptotic value of $\rho(a,b,c)$ is 3, so we will say that an abc-example is good relatively to the Szpiro conjecture if $\rho(a,b,c) \geq 3.8$.

In this paper, we give an algorithm for finding good abc-examples relatively to the abc and the the Szpiro conjectures. Section 2 is a motivation to the algorithm, Section 3 is the General Algorithm, Section 4 and Section 5 indicate how to make the algorithm more efficient, Section 6 is an application of the abc-examples to construct two families of elliptic curves with higher Szpiro ratio (1.2) and Section 7 contains numerical results ralatively to the ratio α and ρ.

N. Elkies and J. Kanapka have computed all good abc-examples with $c \leq 2^{32}$. These results were all given by our algorithm. Furthermore, some good abc-examples with large $c > 2^{32}$ were found. The largest one is

$$109^3.2383^3 + 2^{50}.7^2.17.19.31 = 3^{17}.53^6.193, \quad \alpha = 1.37839, \quad \rho = 3.83622,$$

for which $c = 3^{17}.53^6.193 > 2^{69}$.

II. On a diophantine equation

Our search for good abc-examples is based on solving the diophantine equation

$$ax^n - by^n = cz, \tag{2.1}$$

in relatively prime integers x, y and z, with $x \neq 0$, $y > 0$ and $(c, y) = 1$, where a, b and c are given relatively prime integers with $a > 0$, $b \neq 0$, $c > 0$ and $n \geq 2$ is an integer. We also consider the congruence

$$t^n \equiv ba^{-1} \pmod{c}, \tag{2.2}$$

with $0 \leq t < c$.

Proposition 2.1. *The equation* (2.1) *has a solution with* $(c, y) = 1$ *if and only if the congruence* (2.2) *has a solution. If* (x, y, z) *is a solution of* (2.1) *with* $(c, y) = 1$*, then* $t \equiv xy^{-1} \pmod{c}$*, with* $0 \leq t < c$*, is a solution of the congruence* (2.2) *and there exist integers* u *and* v *such that* $x = tv - cu$ *and* $y = v$*.*

Proof. If (2.1) has a solution with $(y, c) = 1$ then $ax^n - by^n \equiv 0 \pmod{c}$ and $(xy^{-1})^n \equiv ba^{-1} \pmod{c}$. Put $t \equiv xy^{-1} \pmod{c}$ with $0 \leq t < c$. So the congruence (2.2) has a solution and we have $ty \equiv x \pmod{c}$. Then there exists an integer u such that $ty - x = cu$. Hence $x = tv - cu$ with $v = y$.
Conversely if t is a solution of the congruence (2.4) then there exists an integer q such that $at^n - b = cq$. For any relatively prime integers u and v we have

$$a\,(tv - cu)^n - bv^n \equiv (at^n - b)\,v^n \equiv 0 \pmod{c}.$$

Hence $x = tv - cu$, $y = v$ and $z = qv^n + au \sum_{i=1}^{n} (-1)^i \binom{n}{i} (tv)^{n-i} (uc)^{i-1}$ is a solution of (2.3). ■

We now treat the problem of finding solutions x, y and z such that $|z|$ is small. The following theorem guaranties the existence of solutions of the equation (2.1) with small $|z|$.

Theorem 2.1. *If the congruence* (2.2) *is solvable, then the equation* (2.1) *has a solution* $x, y,$ *and* z *with* $|z| < 2\left(\sqrt{a|b|}\right) c^{(n-2)/2}$.

Proof. The linear forms $x = tv - cu$ and $y = v$ have determinant c. Let $l > 0$ be a real number. By Minkowski's theorem, there exist integers u and v, $(u, v) \neq (0, 0)$ such that $|tv - cu| \leq l\sqrt{c}$ and $|v| \leq \sqrt{c}/l$. Then

$$c|z| = |a\,(tv - cu)^n - bv^n| \leq c^{n/2}\left(al^n + \frac{|b|}{l^n}\right).$$

The expression $al^n + \dfrac{|b|}{l^n}$ is minimal when $l = \left(\dfrac{|b|}{a}\right)^{1/2n}$. Taking l equal to this value, we get $|z| < 2\left(\sqrt{a|b|}\right) c^{(n-2)/2}$. ■

We first treat the case where $b < 0$ and n is even.

Theorem 2.2. *Let b and n be as above. If $x \neq 0, y > 0$ and $z = 1$ is a solution of* (2.1) *with $(c, y) = 1$, then there exist a solution t of the congruence* (2.2) *with $0 \leq t < c$ and a convergent $\frac{u}{v}$ of $\frac{t}{c}$ such that $x = tv - cu$ and $y = v$.*

Proof. By proposition 2.1 there exist integers t, u and v such that $0 \leq t < c$, $x = tv - cu$ and $y = v > 0$. As $b < 0$, we have $0 < 2|x|y < x^n + y^n < ax^n - by^n = c$. Then

$$\left|\frac{t}{c} - \frac{u}{v}\right| = \frac{|x|}{cy} < \frac{1}{2y^2} = \frac{1}{2v^2} .$$

It follows [Niven et al. 1991] that $\frac{u}{v}$ is a convergent of $\frac{t}{c}$. ■

Next we treat the case $\{b > 0\}$ or $\{b < 0$ and n is odd$\}$. Let $\delta = \left(\frac{b}{a}\right)^{1/n}$. If $n \geq 3$, we put

$$v_0 = \left(\frac{2^n}{an\delta^{n-1}}\right)^{1/(n-2)} .$$

Theorem 2.3. *Let b and n be as above. Let $x \neq 0$, $y > 0$ and $z = \pm 1$ be a solution of* (2.1). *Put*

$$\varepsilon = \begin{cases} 1 & \text{if } x\delta > 0, \\ -1 & \text{if } x\delta < 0 \text{ and } n \text{ is even}, \\ \cos\dfrac{(n-1)\pi}{n} & \text{if } x\delta < 0 \text{ and } n \text{ is odd}. \end{cases}$$

If $\{n = 2$ and $ab \geq 4\}$ or if $\{n \geq 3$ and $y \geq v_0\}$, then there exist a solution t of the congruence (2.2) *with $0 \leq t < c$ and a convergent $\frac{u}{v}$ in the continued fraction expansion of $\frac{t - \varepsilon\delta}{c}$, if $t - \varepsilon\delta \neq 0$, such that $x = tv - cu$ and $y = v$.*

Proof. We have

$$|x^n - \delta^n y^n| = \prod_{k=0}^{n-1} |x - \theta_k y| ,$$

where $\theta_k = \delta e^{i\frac{2k\pi}{n}}$, $k = 0, \ldots, n-1$. Let k_0 be such that $0 \leq k_0 \leq n-1$ and

$$\left|\frac{x}{y} - \theta_{k_0}\right| = \min_{0 \leq k \leq n-1} \left|\frac{x}{y} - \theta_k\right| .$$

Let ε be as in the theorem. It is easy to see that $\Re e\,(\theta_{k_0}) = \varepsilon\delta$. We have

$$\prod_{k\neq k_0}\left|\frac{x}{y}-\theta_k\right| \geq \frac{1}{2^{n-1}}\prod_{k\neq k_0}\left(\left|\frac{x}{y}-\theta_{k_0}\right|+\left|\frac{x}{y}-\theta_k\right|\right) \geq \frac{1}{2^{n-1}}\prod_{k\neq k_0}|\theta_{k_0}-\theta_k| = \frac{n\delta^{n-1}}{2^{n-1}}.$$

Then

$$\left|\frac{x}{y}-\theta_{k_0}\right| = \frac{c}{a\left|\prod_{k\neq k_0}(x/y-\theta_k)\right| y^n} \leq \frac{2^{n-1}c}{an\delta^{n-1}y^n}\ ,$$

and

$$\left|\frac{x}{y}-\Re e\,(\theta_{k_0})\right| \leq \frac{2^{n-1}c}{an\delta^{n-1}y^n}.$$

By proposition 2.1 there exist integers t, u and v such that $0 \leq t < c$, $x = tv - cu$ and $y = v > 0$. Then

$$\left|\frac{t-\Re e\,(\theta_{k_0})}{c}-\frac{u}{v}\right| \leq \begin{cases} \left(\frac{v_0}{v}\right)^{n-2}\frac{1}{2v^2} & \text{if } n\geq 3, \\ \frac{1}{\sqrt{ab}v^2} & \text{if } \ n=2. \end{cases}$$

If $\{n = 2 \ \text{ and } ab \geq 4\}$ or if $\{n \geq 3 \text{ and } v \geq v_0\}$ then $\left|\frac{t-\Re e\,(\theta_{k_0})}{c}-\frac{u}{v}\right| \leq \frac{1}{2v^2}$ and it follows [Niven et al. 1991] that $\frac{u}{v}$ is a convergent in the continued fraction expansion of $\frac{t-\varepsilon\delta}{c}$.

III. The algorithm

We now describe an algorithm for finding abc-examples and we list those for which $\rho \geq 3.8$ or $\alpha \geq 1.4$. This algorithm is based on solving the diophantine equation (2.1) in integers. Let a, b and c be relatively positive prime integers with $a > 0$, $b \neq 0$ and $c > 0$ and let $n \geq 2$.

The algorithm.

Step 1. Solve the congruence $t^n \equiv ba^{-1} \pmod{c}$. Let $t_j, j = 1, \ldots, r$ be the solutions with $0leqt_j < c$.

Step 2. $j = 1$.

Step 3. $h = 1$.

Step 4. If $h = 1$ then $\varepsilon_h = 1$.
If $h = 2$ then if n is even then $\varepsilon_h = -1$ else $\varepsilon_h = \cos\frac{(n-1)\pi}{n}$.

Step 5. If $t_j - \varepsilon_h \delta = 0$ then goto Step 8 else compute the convergents $\dfrac{u_i}{v_i}$ of $\dfrac{t_j - \varepsilon\delta}{c}$, $i = 1, \ldots, k$, with k so large that $v_k = c$ or $|v_k| > 2^{34}$.
$i = 1$.

Step 6. $X_i = a(t_j v_i - c u_i)^n$, $Y_i = b v_i^n$, $d_i = \gcd(X_i, Y_i)$, $X_i' = X_i/d_i$, $Y_i' = Y_i/d_i$, $Z_i' = X_i' - Y_i'$.
Factor X_i', Y_i' and Z_i' into primes.
Compute the radical G_i of $|X_i'Y_i'Z_i'|$.
Compute $\rho(X_i', Y_i', Z_i')$ and $\alpha(X_i', Y_i', Z_i')$.
If $\rho(X_i', Y_i', Z_i') \geq 3.8$ or $\alpha(X_i', Y_i', Z_i') \geq 1.4$ then print X_i', Y_i', Z_i', $\rho(X_i', Y_i', Z_i')$ and $\alpha(X_i', Y_i', Z_i')$.

Step 7. $i = i + 1$. If $i < k$ then goto Step 6.

Step 8. $h = h + 1$. If $\delta \neq 0$ and $h = 2$ then goto Step 4.

Step 9. $j = j + 1$. If $j \leq r$ then goto Step 3 else stop. ■

In step 1, we have to solve the congruence (2.1). Put $d \equiv ba^{-1} \pmod{c}$ with $0 < d < c$. Let

$$c = \prod_{\substack{p|c \\ p\ prime}} p^e$$

be the factorization of c into primes. The congruence $t^n \equiv d \pmod{c}$ is equivalent to the system

$$t^n \equiv d \pmod{2^e}, \tag{3.1}$$

$$t^n \equiv d \pmod{p^e}, \qquad p|c. \tag{3.2}$$

We solve the system and we apply the Chinese remainder theorem to compute the solutions of the congruence.
First we treat the congruence (3.1). Suppose here that d is odd.
If $e = 0$ or $e = 1$ then $t = 1$ is the solution.
Suppose that $e \geq 2$. Let $n = 2^k m$ with positive integer k and odd m. The number of solutions of (3.1) is $(2, 2^k)(2^k, 2^{e-2}) = 2^\beta$ or zero according as $d \equiv 1 \pmod{2^{\beta+1}}$ or not [Niven et al. 1991]. Assume that $d \equiv 1 \pmod{2^{\beta+1}}$. If $k \geq e - 2$ then $\beta + 1 = e$ and $d \equiv 1 \pmod{2^e}$. Hence the solutions of the congruence (3.1) are the 2^{e-1} odd integers t with $1 \leq t \leq 2^e - 1$. Assume that $k < e - 2$. Then the following procedure computes a solution of (3.1).

Procedure 1.

$t = 1.$
$r = 1 - d.$
$j = \beta + 2.$
while $r \not\equiv 0 \pmod{2^e}$ do
  $t \equiv t - r/2^k \pmod{2^j}.$
  $r = t^n - d.$
  $j = j + 1.$
end.

This procedure terminates with at most $j = e$. The solutions of the congruence (3.1) are $t_j \equiv \pm t + j2^{e-k} \pmod{2^e}$, $j = 0, \ldots, 2^k - 1$.

Next we consider the congruence (3.2). Let $n = p^k m$ with $(m, p) = 1$. The number of solutions of this congruence is $g = (p^k m, p^{e-1}(p-1))$ or zero according as

$$d^{p^{e-1}(p-1)/g} \equiv 1 \pmod{p^e}$$

or not [Niven et al. 1991]. Assume that the congruence (3.2) is solvable. We have $t^n = (t^m)^{p^k}$. Hence we decompose the congruence (3.2) in two congruences

$$l^{p^k} \equiv d \pmod{p^e}, \tag{3.3}$$

with $0 < l < p^e$ and for each solution l

$$t^m \equiv l \pmod{p^e}. \tag{3.4}$$

Considere the congruence (3.3). If $k \geq e - 1$ then

$$l^{p^k} \equiv l^{p^{e-1}} \pmod{p^e}.$$

Put $(p^k, p^{e-1}) = p^\beta$. Then we rewrite (3.3) as

$$l^{p^\beta} \equiv d \pmod{p^e}.$$

It is obvious that $l_0 \equiv d \pmod{p}$, with $0 < l_0 < p$ is a solution of the congruence $l^{p^\beta} \equiv d \pmod{p}$. We use the procedure 2 to compute a solution l of (3.3).

Procedure 2.

$l \equiv d \pmod{p}.$
$r = l^{p^\beta} - d.$

$j = 2.$

while $r \not\equiv 0 \pmod{p^e}$ do

$s \equiv t^{p^\beta - 1})^{-1} \pmod{p}.$

$l \equiv l - rs/p^\beta \pmod{p^j}.$

$r = l^{p^\beta} - d.$

$j = j + 1.$

end.

This procedure terminates with at most $j = e$. Put $(p^k, p^{e-1}) = p^\beta$. The solutions of the congruence (3.3) are $l_j \equiv l + jp^{e-\beta} \pmod{p^e}$, $j = 0, \dots, p^\beta - 1$.
Now consider the congruence (3.4). Let l be a solution of (3.3). Since $(m, p) = 1$, the number of solutions of the congruence (3.4) is $(m, p-1)$. By applying the method described in [Wil-Har] or by varying t from 1 to $p - 1$, we can find all solutions of the congruence $t^m \equiv l \pmod{p}$. Let t_0 be a solution with $0 < t_0 < p$. We compute the solutions of the congruence (3.4) by the procedure

Procedure 3.

$t = t_0.$

$r = t^m - l.$

$j = 2.$

while $r \not\equiv 0 \pmod{p^e}$ do

$s \equiv (mt^{m-1})^{-1} \pmod{p}.$

$t = t - rs \pmod{p^j}.$

$r = t^m - l.$

$j = j + 1.$

end.

This procedure terminates with at most $j = e$. Each solution t_0 gives a solution of the congruence (3.4) and hence a solution of the congruence (3.2). $\blacksquare$

In Step 5, we have to factor many integers into primes. This step in the algorithm is the dominant one. In Step 4, the bound 2^{34} is arbitrary and can be replaced by any other positive integer.

In the next two sections, we prove that the algorithm can be quickened if n is even (Section 4) or if we apply it to special values of c (Section 5). Put

$$\delta = \begin{cases} 0 & \text{if } b < 0 \text{ and } n \text{ is even}, \\ (b/a)^{1/n} & \text{otherwise}. \end{cases} \tag{3.5}$$

Put

$$\varepsilon = \begin{cases} 0 & \text{if } b < 0 \text{ and } n \text{ is even,} \\ \pm 1 & \text{if } b > 0 \text{ and } n \text{ is even,} \\ 1, \cos \dfrac{(n-1)\pi}{n} & \text{if } n \text{ is odd.} \end{cases} \tag{3.6}$$

IV. Relation between t and c-t when n is even

Let $a > 0$, $b \neq 0$ and $c > 0$ be relatively prime integers, and $n \geq 2$. In this section, we assume that n is even. If t is a solution of the congruence (2.2), then $c - t$ is also a solution of the same congruence. The algorithm requires the convergents of the continued fraction expansion of the four real numbers $\dfrac{t - \varepsilon\delta}{c}$ and $\dfrac{c - t - \varepsilon\delta}{c}$ (two if $\delta = 0$) where δ and ε are given by (3.5) and (3.6) respectively. The following theorem shows that we have to consider only the convergents of the continued fraction expansion of two of them (one if $\delta = 0$). Let $[x]$ denote the integer part of the real number x.

Theorem 4.1. *Let the notation be as above. Let $n \geq 2$ be even. Let t, $0 \leq t < \dfrac{c}{2}$ be a solution of the congruence* (2.2). *Let $\xi = \dfrac{t - \varepsilon\delta}{c}$ and $\nu = \xi - [\xi]$.*
(i) *If $\xi \neq 0$ and $\nu \leq 1/2$, then every abc-example found by a convergent of ξ can be found by a convergent of $1 - \xi$.*
(ii) *If $\xi \neq 0$ and $\nu > 1/2$, then every abc-example found by a convergent of $1 - \xi$ can be found by a convergent of ξ.*

Proof. Assume that $\xi \neq 0$. Expand ξ into continued fraction, $\xi = [a_0, a_1, a_2, \ldots]$. We have $a_0 = [\xi]$, and $a_1 = [1/\nu]$. To show (i), assume that $\nu \leq 1/2$. Then $a_1 \geq 2$ and

$$1 - \xi = [-a_0, 1, a_1 - 1, a_2, a_3, \ldots].$$

Let $\dfrac{u_i}{v_i}$ and $\dfrac{u'_i}{v'_i}$, $i = -2, -1, \ldots$ be the convergents of the continued fraction expansion of ξ and $1 - \xi$ respectively. Then for all $i \geq 1$, $u'_i = v_{i-1} - u_{i-1}$ and $v'_i = v_{i-1}$. Let x and y be such that $x = tv_{i-1} - cu_{i-1}$ and $y = v_{i-1}$. Since n is even, we have

$$\begin{aligned} ax^n - by^n &= a\left(tv_{i-1} - cu_{i-1}\right)^n - bv_{i-1}^n \\ &= a\left((c-t)v_{i-1} - c(v_{i-1} - u_{i-1})\right)^n - bv_{i-1}^n \\ &= a\left((c-t)v'_i - cu'_i\right)^n - b{v'}_i^n. \end{aligned}$$

Hence, for $i \geq 1$, every convergent $\dfrac{u_{i-1}}{v_{i-1}}$ of ξ gives the same abc-example as the convergent $\dfrac{u'_i}{v'_i}$ of $1-\xi$. This completes the proof of proof of assertion (i).
To prove (ii), we remark that if $\xi - [\xi] > 1/2$, then $1-\xi-[1-\xi] \leq 1/2$ and hence it suffices to apply (i).

V. Application to special values of c

To find good examples relatively to the abc and the Szpiro conjectures from the expressions

$$ax^n - by^n = cz,$$

it is preferable to choose $c = p^e c'$, where p is a prime, c' is a positive integer satisfying $(p, c') = 1$ and e is a varying integer, simply because:
(i) if the congruence $t^n \equiv ba^{-1} \pmod{p^e c'}$ is solved, then it is easy to solve the congruence $w^n \equiv ba^{-1} \pmod{p^{e+1} c'}$.
(ii) the ratio $\dfrac{\log c}{\log pc'}$ advantages α and ρ.
(iii) the algorithm can be quickened. (Theorem 5.1 and Theorem 5.2 below).

From here until the end of this section, assume that $a > 0$, $b \neq 0$, $c' > 1$, $n \geq 2$, are fixed integers and p is a prime such that $(p, c') = 1$. For all $j \geq 0$, let $c_j = p^j c'$. We say that an example $ax^n - by^n = c_j z$ is found with the triplet (a, b, c_j) if there exist a solution t of the congruence (2.1) and a convergent $\dfrac{u}{v}$ in the continued fraction expansion of a certain real number $\dfrac{t-\varepsilon\delta}{c_j}$ where δ and ε are given by (3.5) and (3.6).

The following theorem shows that we can ignore the convergents $\dfrac{u}{v}$ if $v \equiv 0 \pmod p$.

Theorem 5.1. *Let the notation be as above. Let $e > 0$ be an integer. Assume that the algorithm was applied to all c_j with $0 \leq j < e$. Then every abc-example found with the triplet (a, b, c_e) and a convergent u/v satisfying $v \equiv 0 \pmod p$ was also found with a triplet (a, b, c_j) for some j satisfying $0 \leq j < e$.*

Proof. Let $x \neq 0$, $y > 0$ and z be a solution of (2.1) found with the triplet (a, b, c_e). Let t and $\dfrac{u}{v}$ be as in Proposition 2.1. Assume that $\dfrac{u}{v}$ is a convergent of $\dfrac{t-\varepsilon\delta}{p^e c'}$. Let q be such that $at^n - b = p^e c' q$. We have

$$ax^n - by^n = a\left(tv - p^e c' u\right)^n - bv^n = p^e c' z.$$

If $v = p^{e'} v'$ with $e' > 0$ and $(p, v') = 1$, then

$$a\left(tp^{e'}v' - p^e c' u\right)^n - b\left(p^{e'}v'\right)^n = p^e c' z \tag{5.1}$$

with

$$z = qp^{ne'}v'^n + au\sum_{i=1}^{n}(-1)^i\binom{n}{i}p^{(n-i)e'+(i-1)e}\left(tv'\right)^{n-i}\left(uc'\right)^{i-1}.$$

Let $j = e - \min(e, e')$ and $k = e' - \min(e, e')$. Dividing (5.1) by $p^{\min(ne, ne')}$, we get

$$a\left(tp^k v' - p^j c' u\right)^n - b\left(p^k v'\right)^n \equiv 0 \pmod{p^j c'}. \tag{5.2}$$

The division algorithm gives $t = p^j c' r + t'$, with $0 < t' < p^j c'$. Since $at^n - b \equiv 0 \pmod{p^e c'}$, then $at'^n - b \equiv 0 \pmod{p^j c'}$. Rewrite (5.2) as

$$a\left(t' p^k v' - p^j c'\left(u - rp^k v'\right)\right)^n - bp^k v'^n \equiv 0 \pmod{p^j c'}.$$

Since $\dfrac{u}{v}$ is a convergent of $\dfrac{t - \varepsilon\delta}{p^e c'}$, then

$$\left|\frac{t - \varepsilon\delta}{p^e c'} - \frac{u}{v}\right| < \frac{1}{v^2}\ .$$

That is

$$\left|\frac{p^j c' r + t' - \varepsilon\delta}{p^e c'} - \frac{u}{p^{e'} v'}\right| < \frac{1}{\left(p^{e'} v'\right)^2}\ .$$

Then

$$\left|\frac{t' - \varepsilon\delta}{p^j c'} - \frac{u - rp^k v'}{p^k v'}\right| < \frac{1}{p^{e'+k} v'^2} \le \frac{1}{2v'^2}\ .$$

It follows [Niv et al. 1991] that $\dfrac{u - rp^k v'}{p^k v'}$ is a convergent of $\dfrac{t' - \varepsilon\delta}{p^j c'}$. Hence the convergent $\dfrac{u}{v}$ of $\dfrac{t - \varepsilon\delta}{p^e c'}$ gives the same example as the convergent $\dfrac{u - rp^k v'}{p^k v'}$ of $\dfrac{t' - \varepsilon\delta}{p^j c'}$ with $j < e$. ■

The following theorem shows that we can ignore in the algorithm the solutions (x, y, z) of the equation (2.1) satisfying $z \equiv 0 \pmod{p}$ if $c = p^e c'$.

Theorem 5.2. *Let the notation be as in Theorem* 5.1. *Let e be an integer. Then every solution (x, y, z) of the equation* (2.1) *satisfying $z \equiv 0 \pmod{p}$ found with the triplet (a, b, c_e) is also found with a triplet (a, b, c_j) for some j satisfying $j > e$.*

Proof. Let $x \neq 0$, $y > 0$, $z \neq 0$ be a solution of the equation (2.1). By Theorem 5.1 we assume that $(y, pc') = 1$. Let t, u and v be as in Proposition 2.1. Assume that $\dfrac{u}{v}$ is a convergent of $\dfrac{t - \varepsilon\delta}{p^e c'}$. If $z = p^{e'} z'$ with $e' > 0$ and $(p, z') = 1$, then $ax^n - by^n = p^{e+e'} c' z'$.

By Proposition 2.1, there exist integers u', v' and t' such that $t'^n \equiv ba^{-1} \pmod{p^{e+e'}c'}$, $0 < t' < p^{e+e'}c'$, $x = t'v' - p^{e+e'}c'u'$ and $y = v'$. Then $y = v = v'$ and $x = t'v - p^{e+e'}c'u' = tv - p^e c'u$. Hence

$$(t' - t)v = p^e c'(p^{e'}u' - u).$$

Since $(v, pc') = 1$, there exists an integer r such that $p^{e'}u' - u = rv$ and $t' - t = rp^e c'$. Then

$$\begin{aligned}\left|\frac{u'}{v'} - \frac{t' - \varepsilon\delta}{p^{e+e'}c'}\right| &= \left|\frac{u + rv}{p^{e'}v} - \frac{rp^e c' + t - \varepsilon\delta}{p^{e+e'}c'}\right| \\ &= \frac{1}{p^{e'}}\left|\frac{u}{v} - \frac{t - \varepsilon\delta}{p^e c'}\right| \le \frac{1}{p^{e'}v^2} \le \frac{1}{2v^2}\ .\end{aligned}$$

It follows [Niven et al. 1991] that $\dfrac{u'}{v'}$ is a convergent of $\dfrac{t' - \varepsilon\delta}{p^{e+e'}c'}$ with $e + e' > e$. ■

ACKNOWLEDGMENTS

I wish to thank Professor Y. Hellegouarch for his encouragement and J. Browkin and J. Brzezinski for sending me their examples.

REFERENCES

[Browkin, Brzezinski 1992] J. Browkin and J. Brzezinski, "Some remarks on *abc*-conjecture", preprint Univ. Göteborg (Sweden) ,1992-30.

[Nitaj 1992] A. Nitaj, "Algorithms for finding *abc*-examples", preprint Univ. Caen (France) **60**, 1992.

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

[Oesterlé 1988] 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.

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

[de Weger 1987] B. M. M. de Weger, "Solving exponential diophantine equations using latice basis reduction algoritms", *J. Number Theory* **26** (1987), 325-367.

CHAPITRE 4

Résultats expérimentaux

Résultats expérimentaux

I. Quelques estimations pour la conjecture abc

Soient a, b et c des entiers positifs tels que $a < b < c$ et $a + b = c$. J. Oesterlé avait proposé deux formules pour majorer c en fonction de $r(abc)$, radical de abc. La première estimation était:

$$c \leq r^{1+4(1+2/\log\log r)/\left(\sqrt{\log r}\log\log r\right)}, \tag{1}$$

où $r = r(abc)$, en précisant que les constantes 4 et 2 ne peuvent pas être diminuées. Cette inégalité implique que la quantité τ définie par:

$$\tau = \tau(a,b,c) = 1 + \frac{4}{\sqrt{\log r}\log\log r}\left(1 + \frac{2}{\log\log r}\right) - \frac{\log c}{\log r},$$

est positive. On sait maintenant que l'estimation (1) est fausse car nous avons déterminé les contre-exemples listés dans la table 1 suivante.

Table 1

a	b	c	τ
$11^3.19^7.21023^3$	$3^{34}.1945713113$	$2^{43}.5^{10}.17.31^3$	-0.04060
$2^{42}.7^6.13^3.53^3$	$5.11^{20}.179471$	$3.79.148296823^3$	-0.02903
$2^{20}.7^{18}.127^3$	$31.53^4.1873133^3$	$3^{39}.11.191.599597$	-0.02807
$3.31.773^2$	$5^8.11^4.103^2.113^3$	$2.19^{11}.613^2$	-0.02670
$37.73^2.4817^4$	$2^{20}.5^3.7^2.19$	$3^2.23^2.29^{10}.53$	-0.01594
$7^4.151^2.181^4$	$2^{25}.3^4.29.10753$	5^{24}	-0.00858
$3^8.10753^2$	$5^{12}.7^2.151.181^2$	$2^{46}.29^2$	-0.00833
$7^2.23^2$	$2^{12}.3.5.11.19^4.29.167^2$	$31^8.17^4$	-0.00156

J. Oesterlé a ensuite proposé l'estimation suivante:

$$abc \leq r^{3+12(1+2/\log\log r)/\left(\sqrt{\log r}\log\log r\right)}, \tag{2}$$

où r désigne toujours $r(abc)$. Cette inégalité implique de même que la quantité τ' définie par:

$$\tau' = \tau'(a,b,c) = 3 + \frac{12}{\sqrt{\log r}\log\log r}\left(1 + \frac{2}{\log\log r}\right) - \frac{\log(abc)}{\log r},$$

est positive. Nous avons aussi découvert les contres exemples de la table 2 ci-dessous.

Table 2

a	b	c	τ'
$11^3.19^7.21023^3$	$3^{34}.1945713113$	$2^{43}.5^{10}.17.31^3$	-0.08593
$2^{20}.7^{18}.127^3$	$31.53^4.1873133^3$	$3^{39}.11.191.599597$	-0.05438
$2^{42}.7^6.13^3.53^3$	$3.79.148296823^3$	$5.11^{20}.179471$	-0.05146

II. Etude des rapports de Szpiro et d'Oesterlé-Masser

Rappelons que pour toute relation abc, écrite sous la forme $a+b=c$, avec $0 < a < b < c$ et $(a,b) = 1$, le rapport $\alpha(a,b,c)$ d'Oesterlé-Masser et le rapport $\rho(a,b,c)$ de Szpiro sont définis respectivement par:

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

et

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

Il est clair alors que pour toute relation abc, ces rapports sont liés par la double inégalité:

$$\alpha < \rho < 3\alpha.$$

Ainsi, si on admet la conjecture abc ou les conjectures de Szpiro, ces deux rapports sont bornés (voir Chapitre 1, parties I et II).

Nous donnons maintenant une méthode pour déterminer des familles infinies de triplets (a,b,c) pour lesquels $\alpha(a,b,c) > 1$ et $\rho(a,b,c) > 3$. Soient A un entier non nul sans facteurs cubiques et x_0, y_0 et z_0 trois entiers vérifiant $(x_0, y_0) = 1$ et:

$$x_0^3 + y_0^3 = Az_0^3.$$

Pour tout $n \geq 1$, on définit x_n, y_n et z_n par les formules suivantes, obtenues par duplication cubique (appelée aussi méthode de Fermat ou de la tangente à une courbe elliptique):

$$\left\{ \begin{aligned} x_n &= x_{n-1}\left(x_{n-1}^3 + 2y_{n-1}^3\right), \\ y_n &= -y_{n-1}\left(2x_{n-1}^3 + y_{n-1}^3\right), \\ z_n &= z_{n-1}\left(x_{n-1}^3 - y_{n-1}^3\right). \end{aligned} \right. \tag{3}$$

Alors on a pour tout $n \geq 0$:

$$x_n^3 + y_n^3 = Az_n^3.$$

Proposition 1. *Si les entiers x_0 et y_0 vérifient $x_0 \equiv 2 \pmod 3$ et $y_0 \equiv 1 \pmod 3$, alors pour tout $n \geq 0$, $(x_n, y_n) = 1$, $z_n \neq 0$ et $\lim_{n\to\infty} |z_n| = +\infty$.*

Preuve. Remarquons d'abord que pour tout $n \geq 0$, $x_n \equiv 2 \pmod 3$ et $y_n \equiv 1 \pmod 3$. Montrons maintenant que $(x_n, y_n) = 1$ pour tout $n \geq 0$. C'est le cas pour $n = 0$. Supposons que $(x_n, y_n) = 1$. Soit p un diviseur premier de (x_{n+1}, y_{n+1}) avec $x_{n+1} = x_n(x_n^3 + 2y_n^3)$ et $y_{n+1} = -y_n(2x_n^3 + y_n^3)$. Si p divise x_n, alors p ne divise ni y_n, ni $2x_n^3 + y_n^3$. Si p divise $x_n^3 + 2y_n^3$, alors il ne divise pas y_n. La relation $2(x_n^3 + 2y_n^3) = 2x_n^3 + y_n^3 + 3y_n^3$ implique que si p divise $x_n^3 + 2y_n^3$ et $2x_n^3 + y_n^3$, alors il divise $3y_n^3$ et donc $p = 3$. Ainsi 3 divise $x_n^3 + 2y_n^3$, ce qui contredit la congruence $x_n^3 + 2y_n^3 \equiv 1 \pmod 3$. Alors $(x_{n+1}, y_{n+1}) = 1$. Ainsi z_n n'est jamais nul. D'autre part, l'un des trois entiers x_0, y_0 ou Az_0 est pair, x_0 par exemple. Alors $x_1 = x_0(x_0^3 + 2y_0^3)$ est divisible par 2^2 et par récurrence, x_n est divisible par 2^{n+1} pour tout $n \geq 2$. Ceci donne la conclusion de la proposition. ■

Proposition 2. *Soit A un entier sans facteurs cubiques. Soient $x_0 \equiv 2 \pmod 3$, $y_0 \equiv 1 \pmod 3$ et z_0 des entiers vérifiant $x_0^3 + y_0^3 = Az_0^3$ et x_n, y_n, z_n définis par les relations (3). Pour tout $n \geq 0$, soient $a_n = \min(|x_n|^3, |y_n|^3, |Az_n^3|)$, $c_n = \max(|x_n|^3, |y_n|^3, |Az_n^3|)$ et $b_n = c_n - a_n$. Il existe alors un entier $n_0 \geq 0$ tel que pour tout $n \geq n_0$, on ait:*

$$\alpha(a_n, b_n, c_n) = \frac{\log c_n}{\log r(a_n b_n c_n)} > 1,$$

et

$$\rho(a_n, b_n, c_n) = \frac{\log a_n b_n c_n}{\log r(a_n b_n c_n)} > 3.$$

Preuve. La proposition 1 montre que les triplets (a_n, b_n, c_n) sont formés d'entiers premiers entre eux vérifiants $0 < a_n < b_n$ et $a_n + b_n = c_n$ et qu'ils sont en nombre infini. De plus pour tout $n \geq 1$, $a_n b_n c_n$ est divisible par 2^{3n}. Soit n_0 un entier tel que $(r(2A))^3 < 2^{3n_0}|A|$. Alors pour pour tout $n \geq n_0$ on a:

$$r(a_n b_n c_n) = r\left(\frac{|x_n y_n z_n|^3}{2^{3n}} 2^{3n} A\right) < (a_n b_n c_n)^{1/3} < c_n.$$

Ceci donne les inégalités de la proposition. ∎

Remarques.
(i) Les familles construites selon le modèle ci-dessus permettent aussi de montrer que la constante $c(\varepsilon)$ qui correspond à ε dans les conjectures *abc* et de Szpiro est telle que $\lim_{\varepsilon \to 0} c(\varepsilon) = +\infty$.
(ii) On peut étendre les familles construites ci-dessus en des familles quelconques issues de relations $ax_0^3 + by_0^3 + cz_0^3 = 0$.

Proposition 3. *Soit (a, b, c) un triplet d'entiers formant une relation abc. Il existe au plus un nombre fini de relations abc admettant le même rapport α que le triplet (a, b, c).*

Preuve. Soit (a, b, c) un triplet formant une relation *abc*. Soit (x, y, z) un triplet d'entiers premiers entre eux vérifiant $x + y = z$, $0 < x < y < z$ et tels que $\alpha(x, y, z) = \alpha(a, b, c)$. Alors

$$z = c^{\log r(xyz)/\log r(abc)}.$$

Cette égalité n'est possible que si $\log r(xyz) = \log r(abc)$ et donc $z = c$ et $r(xy) = r(ab)$. En particulier $x + y = c$, et d'après le théorème de Mahler, cette équation n'admet qu'un nombre fini de solutions. ∎

Remarques.
(i) Il existe des triplets (a, b, c) qui n'ont pas d'autres représentants du même rapport $\alpha(a, b, c)$. Un exemple évident est le triplet $(3, 5, 8)$.

(ii) Soit $n \geq 2$ un entier. On définit les triplets (a_n, b_n, c_n) et (x_n, y_n, z_n) par:

$$a_n = 2\left(2^{n-1} - 1\right), b_n = \left(2^n - 1\right)^2, c_n = a_n + b_n,$$
$$x_n = 2^n - 1, y_n = 2^{n+1}\left(2^{n-1} - 1\right), z_n = x_n + y_n.$$

Alors $c_n = z_n$, $r(a_n b_n) = r(x_n y_n)$ et donc on a:

$$\alpha(a_n, b_n, c_n) = \alpha(x_n, y_n, z_n).$$

On a vu précédemment que la conjecture *abc* implique que le rapport α est borné. Plus précisement, on a la proposition suivante.

Proposition 4. *La conjecture abc implique qu'il existe une relation abc pour laquelle le rapport α est maximal.*

Preuve. Admettons la conjecture *abc*. Supposons qu'il n'existe pas de relations *abc* admettant un rapport α maximal. Soit (a_0, b_0, c_0) une relation *abc* 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, $\lim\limits_{n \to \infty} r(a_n b_n c_n) = \infty$ 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. ■

Remarque. La démonstration de la proposition 4 implique que pour toute relation (a, b, c) avec $\alpha(a, b, c) > 1$, il n'existe qu'un nombre fini de relations *abc* admettant un meilleur rapport α.

En utilisant une démonstration similaire à celle de la proposition 4, on a:

Proposition 5. *La conjecture abc implique qu'il existe une relation abc pour laquelle le rapport ρ est maximal.*

III. Architecture des bonnes relations *abc*

Une vision rapide sur les bonnes relations *abc* des tables 3 et 4 montre que chacune de ces relations contient un exposant égal à 1, sauf quelques relations où le plus petit exposant qui apparaît est 2. On peut alors se poser la question suvante:
"y a-t-il des relation abc (bonnes ou pas) dans lesquelles le plus petit exposant est 3, 4 ou plus?"
Nous verrons comment la conjecture *abc* peut répondre à cette question. Donnons d'abord une définition.

Définition 1. *Soit $n \geq 2$ un entier. Un entier $x > 0$ est dit n-puissant si tout nombre premier p divisant x est tel que $p^n | x$.*

La question ci-dessus devient maintenant:
"Soit $n \geq 2$ un entier. L'équation diophantienne $x+y=z$ admet-elle des solutions en entiers n-puissants?"

(a). Cas $n=2$. L'équation ci dessus admet plusieurs familles de solutions infinies. Citons en quelques unes.

(i) Soient u et v deux entiers premiers entre eux. On définit les entiers de Pythagore $x(u,v)$, $y(u,v)$ et $z(u,v)$ par:

$$\begin{aligned} x(u,v) &= 2^2u^2v^2, \\ y(u,v) &= (u-v)^2, \\ z(u,v) &= \left(u^2+v^2\right)^2. \end{aligned}$$

Alors $x(u,v)$, $y(u,v)$ et $z(u,v)$ sont une réponse pour la question avec $n=2$.

(ii) Soient u et v deux entiers premiers entre eux. On définit les entiers $x(u,v)$, $y(u,v)$ et $z(u,v)$ par:

$$\begin{aligned} x(u,v) &= 3^3\left(\frac{uv(u+v)}{2}\right)^2, \\ y(u,v) &= \left(\frac{(u-v)(u+2v)(2u+v)}{2}\right)^2, \\ z(u,v) &= \left(u^2+uv+v^2\right)^3. \end{aligned}$$

Alors $x(u,v)$, $y(u,v)$ et $z(u,v)$ sont une une réponse pour la question avec $n=2$.

(iii) Définissons les suites (x_k), (y_k) et $z_k)$ par $x_0=2$, $y_0=1$ et $z_0=1$ et par les relations de récurrences (3). Alors x_k, y_k et z_k vérifient:

$$x_k^3+y_k^3=3^2z_k^3$$

et sont donc une une réponse pour la question avec $n=2$.

(b). Cas $n=3$. Une seule solution était connue pour l'équation correspondante (voir [Bro-Brz]):

$$271^3+2^3\cdot 3^5\cdot 73^3=919^3.$$

D'autre part, P. Erdös avait proposé la conjecture suivante (voir [Guy], B 16):

Conjecture 1. (Erdös). *Il existe une infinité de triplets 3-puissants (x,y,z) premiers entre eux tels que $x+y=z$.*

Nous donnons ci dessous trois familles infinies de triplets 3-puissants répondant à la conjecture d'Erdös. Ces familles sont construites par les relations (3) à partir de relations du genre $x_0^3 + y_0^3 = Az_0^3$ où $r(A)|r(z_0)$. C'est le cas pour les relations:

$$17^3.106219^3 - 37^3.197^3.307^3 = -2^7.3^4.5^3.7^3.2287^3,$$
$$-271^3 + 919^3 = 2^3.3^5.73^3,$$
$$89^3.307^3.2341^3 - 17^3.19^3.83341^3 = 2^5.3^4.7^3.13^3.9973^3.$$

(c). Cas $n = 4$. Pour $n = 4$, aucune réponse n'est connue. P. Erdös conjecture qu'il n'y a qu'un nombre fini de solutions (voir aussi [Guy], B 16)). La même conclusion peut être obtenue comme conséquence de la conjecture *abc*:

Proposition 6. *La conjecture abc implique qu'il n'y a qu'un nombre fini de triplets (x, y, z) d'entiers 4-puissants premiers entre eux tels que $x + y = z$.*

Preuve. Appliquons la conjecture *abc* au triplet (x, y, z). On obtient:

$$z \leq c(\varepsilon)(xyz)^{(1+\varepsilon)/4} \leq c(\varepsilon)z^{3(1+\varepsilon)/4}.$$

Alors

$$z^{1-3(1+\varepsilon)/4} \leq c(\varepsilon),$$

et donc que z est borné. ■

(d) Pour $n \geq 5$, nous avons le résultat suivant, qui s'appuie sur l'exemple d'E. Reyssat, qui est le meilleur exemple connu actuellement pour la conjecture *abc*:

$$2 + 3^{10} \cdot 109 = 23^5, \quad \alpha_0 = 1.62991.$$

Proposition 7. *Si la conjecture abc est vraie et si l'exemple de Reyssat est le meilleur pour la conjecture abc, alors il n'existe pas de triplet (x, y, z) d'entiers positifs n-puissants premiers entre eux et vérifiant $x + y = z$ pour $n \geq 5$.*

Preuve. Si (x, y, z) est un triplet *abc* tel que x, y et z sont n-puissant, alors:

$$r(xyz) \leq (xyz)^{1/n},$$

et donc:

$$n \leq \frac{\log(xyz)}{\log r(xyz)} \leq 3\alpha_0 < 5,$$

ce qui termine la preuve. ■

IV. Application des algorithmes

Dans leur principe, les algorithmes de détermination des bonnes relations abc, décrits dans le chapitre 3 sont efficaces et ne posent aucune difficulté. Tel devrait être le cas si on dispose d'un moyen rapide de factorisation des entiers. En effet l'étape dominante de ces algorithmes consiste en la factorisation des entiers x, y et z obtenus en prenant $x = tv - cu$, $y = v$, $z = (ax^n - by^n)/c$, où a, b, c et n sont des entiers donnés et t est une solution de la congruence $t^n \equiv ba^{-1} \pmod{c}$ et où finalement u et v sont tels que u/v est une réduite de l'expansion de $(t - (b/a)^{1/n})/c$ en fraction continue. A défaut d'une méthode assez rapide de factorisation des entiers, nous avons utilisé tout simplement la méthode du crible d'Erathostène en nous limitant aux nombres premiers inférieurs à 300. La plupart de nos bonnes relations abc figurant dans les tables 3 et 4 à la fin de ce chapitre contiennent des facteurs premiers inférieurs à 300. Plus exactement, nous avons les résultats suivants:

- Pour la table 1, le pourcentage des bonnes relations obtenues avec x ou y contenant des facteurs supérieurs à 301 est de 8/100. On remarque aussi que la première de ces relations se trouve à la 11^{eme} place.

- Pour la table 2, ce pourcentage est de 8/100 et la première de ces relations apparaît à la 28^{eme} place.

On remarque que le pourcentage des bonnes relations abc formées de x ou de y contenant des facteurs supérieurs à 300, obtenues par les algorithmes est le même pour les deux tables 3 et 4.
Les bonnes relations de ces deux tables ont été obtenues avec les bornes suivantes pour a, b, c et n.

(i) $n = 2$, $1 \leq a \leq |b| \leq 300$ avec $b < 0$, $c = p^e$ où p est un nombre premier satisfaisant $2 \leq p \leq 31$ et e est un entier positif tel que $p^e \leq 2^{60}$ [Nit1].

(ii) $n = 2$, $1 \leq a \leq b \leq 300$, $c = p^e$ où p est un nombre premier satisfaisant $2 \leq p \leq 31$ et e est un entier positif tel que $p^e \leq 2^{40}$ [Nit1].

(iii) $n = 3, 5$, $1 \leq a \leq b \leq 200$, $c = p^e$ où p est un nombre premier satisfaisant $2 \leq p \leq 31$ et e est un entier tel que $p^e \leq 2^{40}$.

Nos algorithmes ont ainsi déterminés 103 relations abc vérifiant $\rho(a, b, c) \geq 3.8$ et 86 relations avec $\alpha(a, b, c) \geq 1.4$.

Il est clair que les exemples des tables 3 et 4 ont été obtenus d'une façon particulière et que ces tables ne sont complètes dans aucun sens, c'est à dire qu'il existe peut être de bonnes relations abc qui sont inférieures à la plus grande relation de ces tables, mais qui n'y figurent pas.

V. Tables des bonnes relations abc

Dans cette partie, nous avons listé, avec leur auteurs, toutes les bonnes relations $X+Y=Z$ avec $(X,Y,Z)=1$ et $0<X<Y<Z$ relativement à α et ρ dans la tables 3 et la table 4 respectivement. Quelques exemples (indiqués avec un astérisque) n'ont pas été déterminés par nos algorithmes. D'autre part, plusieur exemples ont été découverts en même temps, mais indépendamment par J. Browkin et J. Brzezinski. Ces exemples sont indiqués par les initiales B-B (voir [Bro-Brz]).

L'algorithme de Browkin et de Brzezinski utilise aussi des méthodes d'approximation. Plus précisement, étant donnés un entier $n \geq 2$ et un entier positif a, l'algorithme consiste à déterminer des réduites p/q du développement de $a^{1/n}$ en fraction continue, en prenant $x = min(p^n, aq^n, |p^n - aq^n|$, $z = max(p^n, aq^n, |p^n - aq^n|$ et $y = z - x$, on obtient une relation, qui en la simplifiant donnera une relation abc. La suite se borne alors à calculer les valeurs de $\alpha(x,y,z)$ et $\rho(x,y,z)$.

Table 3

Nr	X	Y	Z	α	First author
1)	2	$3^{10}.109$	23^{5}	1.62991	E. Reyssat
2)	11^{2}	$3^{2}.5^{6}.7^{3}$	$2^{21}.23$	1.62599	B.M.M. de Weger
3)*	19.1307	$7.29^{2}.31^{8}$	$2^{8}.3^{22}.5^{4}$	1.62349	B-B
4)	283	$5^{11}.13^{2}$	$2^{8}.3^{8}.17^{3}$	1.58076	B-B, A. Nitaj
5)	1	2.3^{7}	$5^{4}.7$	1.56789	B.M.M. de Weger
6)	7^{3}	3^{10}	$2^{11}.29$	1.54708	B.M.M. de Weger
7)	13.19^{6}	$2^{30}.5$	$3^{13}.11^{2}.31$	1.52700	A. Nitaj
8)	239	$5^{8}.17^{3}$	$2^{10}.37^{4}$	1.50284	B-B, A. Nitaj
9)	$5^{2}.7937$	7^{13}	$2^{18}.3^{7}.13^{2}$	1.49762	B.M.M. de Weger
10)	$2^{2}.11$	$3^{2}.13^{10}.17.151.4423$	$5^{9}.139^{6}$	1.49243	A. Nitaj
11)	73	$2^{13}.7^{7}.941^{2}$	$3^{16}.103^{3}.127$	1.49159	A. Nitaj
12)	11^{2}	$3^{9}.13$	$2^{11}.5^{3}$	1.48887	B.M.M. de Weger
13)	37	2^{15}	$3^{8}.5$	1.48291	B.M.M. de Weger
14)	1	$3^{16}.7$	$2^{3}.11.23.53^{3}$	1.47445	A. Nitaj
15)	7^{2}	$2^{10}.11.53^{2}$	$3^{4}.5^{8}$	1.47414	B-B, A. Nitaj
16)	$3^{4}.199$	11^{8}	$2^{3}.5^{7}.7^{3}$	1.47130	B-B, A. Nitaj
17)	$2^{7}.5^{2}$	$7^{6}.41$	13^{6}	1.46192	B.M.M. de Weger
18)	$3^{2}.5^{2}$	$2^{4}.17^{3}.31^{4}$	$7^{10}.257$	1.45707	A. Nitaj
19)	1	$2^{5}.3.5^{2}$	7^{4}	1.45567	B.M.M. de Weger
20)	$3^{2}.11^{6}$	2^{35}	$19^{5}.13883$	1.45513	B-B
21)	$2^{19}.13.103$	7^{11}	$3^{11}.5^{3}.11^{2}$	1.45261	B.M.M. de Weger
22)	$3^{5}.7$	$5^{6}.67$	2^{20}	1.45134	B-B, A. Nitaj
23)	$3^{5}.7^{3}$	$2^{13}.23^{3}.59$	$5^{3}.19^{6}$	1.45086	B-B
24)	1	$3^{3}.5^{3}.7^{7}.23$	$2^{13}.11^{4}.13.41$	1.45003	A. Nitaj

Table 3 (continued)

Nr	X	Y	Z	α	First author
25)	1	$3.5^5.47^2$	$2^{18}.79$	1.44965	G. Frey
26)	$11^2.43$	$5^9.7^2.13^4.97$	$2^3.3.73^7$	1.44798	A. Nitaj
27)	89	7.11^8	$2^{20}.3^3.53$	1.44774	A. Nitaj
28)	$3^2.5^7.79$	$2^{29}.13$	$11^7.19^2$	1.44625	A. Nitaj
29)	2.13^2	5^8	3.19^4	1.44506	B-B, A. Nitaj
30)	1	$2^{12}.5^3$	$3^5.7^2.43$	1.44331	B.M.M. de Weger
31)	$3^2.19^3$	5^{11}	$2^{17}.373$	1.44328	B-B, A. Nitaj
32)	31^3	$2.17.41^5$	$3.5^7.7^5$	1.44144	A. Nitaj
33)	$3^4.23^2$	31^5	$2^{15}.5^3.7$	1.44097	B-B, A. Nitaj
34)	1	$2^4.3^7.547$	$5^8.7^2$	1.43906	B.M.M. de Weger
35)*	1	19.509^3	$2^{19}.3^4.59$	1.43836	B-B
36)	2.13^5	$7^6.173^2$	$3^{13}.47^2$	1.43618	A. Nitaj
37)	$2^{10}.7$	5^7	$3^8.13$	1.43501	B.M.M. de Weger
38)	$2^5.3^{18}$	$5^6.7^{10}.23^2$	$11^9.990203$	1.43346	A. Nitaj
39)	31^2	$3^5.5^9$	$2^5.23^4.53$	1.43304	B-B, A. Nitaj
40)	2^{21}	$7^6.17.8209^2$	$5^{12}.743^2$	1.43290	A. Nitaj
41)	$2^9.19^2$	$59^6.73$	$3^3.5^7.7^2.31^3$	1.43109	A. Nitaj
42)	193	$2.5^6.19^2.1193^2$	$3^9.13^8$	1.43042	A. Nitaj
43)	$3^6.7^2.13.127^2$	$2^{38}.61.137$	$5^{11}.19^6$	1.43018	B-B
44)	$3^9.29$	$7^6.43^2$	$2^{24}.13$	1.42955	A. Nitaj
45)	3^{21}	$7^2.11^6.199$	$2.13^8.17$	1.42907	A. Nitaj
46)	73^2	$2^{11}.11^4.13^3$	$3^{11}.5^5.7.17$	1.42891	B-B
47)	11	$7^3.167^2$	2.3^{14}	1.42832	B-B, A. Nitaj
48)	73	$11^5.157^2$	$2^2.3^{10}.7^5$	1.42757	B-B, A. Nitaj

Table 3 (continued)

Nr	X	Y	Z	α	First author
49)	61^4	$2^{20}.41^3.83^2$	$3^{22}.5.19.167$	1.42749	A. Nitaj
50)	3^{10}	$7^8.23$	$2^9.509^2$	1.42712	A. Nitaj
51)	31	$2^5.5^{10}.19^2$	$3.7^5.11^3.41^2$	1.42675	B-B, A. Nitaj
52)	3	5^3	2^7	1.42657	B.M.M. de Weger
53)	$5^2.11$	$13^3.1483^2$	$2^{29}.3^2$	1.42338	B-B, A. Nitaj
54)	$2^4.59$	$5^{12}.19$	$3^3.11^2.17^5$	1.42183	B-B, A. Nitaj
55)	5^7	$11^5.13^2$	$2^{15}.7^2.17$	1.42158	A. Nitaj
56)	$2^9.37^3.89$	$3^9.5^9.31$	103^6	1.42101	A. Nitaj
57)	$7^8.19$	$2^{15}.5^2.37^2$	3.17^7	1.42044	A. Nitaj
58)	23^3	$3^9.5^7.31$	$2^7.7^3.13.17^4$	1.42004	A. Nitaj
59)	7^2	$2^{17}.181^2$	$3^8.809^2$	1.41892	B-B, A. Nitaj
60)*	13.3499	2^{39}	$3^4.5^{11}.139$	1.41823	B-B
61)*	$5^6.1609$	$2^9.3^{14}.13^3$	1523^4	1.41763	B-B
62)	$3^9.43^3$	$5^{13}.5323$	$2^7.7^3.23^6$	1.41679	A. Nitaj
63)*	$41^4.33941$	$3^{12}.19^7$	$2^{23}.5^9.29$	1.41644	B-B
64)	$3.5^4.599$	11.23^8	$2^{22}.59^3$	1.41605	B-B, A. Nitaj
65)	7^3	$5^{13}.181$	$2^4.3.11.13^2.19^5$	1.41556	A. Nitaj
66)	$3^{11}.5^4$	$7.11^6.43$	$2^{17}.17^3$	1.41450	G. Xiao
67)	$2^6.5.137$	3^{14}	13^6	1.41370	B-B, A. Nitaj
68)	5^2	$3^7.13^3$	$2^8.137^2$	1.41328	B-B, A. Nitaj
69)	$3^6.157^3.283$	23^{10}	$2^{30}.5^2.11^2.13$	1.41317	B-B, A. Nitaj
70)	5	3^{11}	$2^{10}.173$	1.41268	B.M.M. de Weger
71)	79^3	$3^6.7.11.13^5$	$2^{18}.43^3$	1.41168	A. Nitaj
72)	$3.13^2.1049$	$2^{39}.29^2.107$	$19^3.139^6$	1.41161	B-B, A. Nitaj

Table 3 (continued)

Nr	X	Y	Z	α	First author
73)*	$67^2.2399$	$3^{13}.107^3$	$2^6.5^{15}$	1.41068	B-B
74)	$2^{13}.3^{13}.11^3$	$13.29.43^6.673$	$5^{20}.17$	1.41004	A. Nitaj
75)	7^2	83^5	$2^2.3^{12}.17.109$	1.40897	B-B, A. Nitaj
76)	$2^2.13$	$7^3.41^5.181$	$3^{14}.5.67^3$	1.40779	A. Nitaj
77)	$3^2.233$	$23^7.293^2$	$2^{15}.5^2.13^5.31^2$	1.40740	A. Nitaj
78)*	241	$2^{12}.3^4.5^6.1181$	$11^8.13^4$	1.40721	B-B
79)	$3^9.163$	$2^3.11^6.17$	5^{12}	1.40705	B-B, A. Nitaj
80)	7^9	$3^2.5^7.13^3$	$2^{16}.19^2.67$	1.40652	J. Kanapka
81)	$2^{19}.367^3$	$5^{17}.197.281$	$13^2.251^6$	1.40642	A. Nitaj
82)	$2^{16}.41.71$	$3^{15}.7^2$	19^7	1.40610	A. Nitaj
83)	5.7^2	$13^2.43^3$	$2^{11}.3^8$	1.40608	B-B, A. Nitaj
84)	13^3	$2^9.37^2$	$3^2.5^7$	1.40578	A. Nitaj
85)	$2^{24}.3^5$	$5.19^5.59^2$	$7^{10}.167$	1.40544	A. Nitaj
86)	631	$2^{26}.5.29^2$	$3^3.7^{10}.37$	1.40448	A. Nitaj
87)	1	$3^9.7^2.197$	$2^7.5^7.19$	1.40426	A. Nitaj
88)	$3^3.13$	$2^5.11.19^2.73^3$	$5^2.7^{11}$	1.40348	A. Nitaj
89)	$3^{12}.5^6$	$31^2.7^9$	$2^9.11^5.571$	1.40218	A. Nitaj
90)	$2^{33}.5$	$3^9.7^6.31^2.97$	$11^2.19^3.127^4$	1.40198	A. Nitaj

Table 4

Nr	X	Y	Z	ρ	First author
1)	13.19^6	$2^{30}.5$	$3^{13}.11^2.31$	4.41901	A. Nitaj
2)	$2^{19}.13.103$	7^{11}	$3^{11}.5^3.11^2$	4.24789	B.M.M. de Weger
3)	3^{21}	$7^2.11^6.199$	$2.13^8.17$	4.20094	A. Nitaj
4)	$7.11^6.43$	$3^{11}.5^4$	$2^{17}.17^3$	4.10757	G. Xiao
5)	$2^{16}.41.71$	$3^{15}.7^2$	19^7	4.09655	A. Nitaj
6)	$3^{12}.5^6$	$7^9.31^2$	$2^9.11^5.571$	4.09647	A. Nitaj
7)	$7^8.19$	$2^{15}.5^2.37^2$	3.17^7	4.09080	A. Nitaj
8)	$2^{24}.3^5$	$5.19^5.59^2$	$7^{10}.167$	4.07114	A. Nitaj
9)	$3^6.157^3.283$	23^{10}	$2^{30}.5^2.11^2.13$	4.05990	B-B, A. Nitaj
10)	$2^{13}.3^{13}.11^3$	$13.29.43^6.673$	$5^{20}.17$	4.04710	A. Nitaj
11)	$5^{13}.13$	$2^{17}.19^3.23$	$3^{17}.283$	4.04498	A. Nitaj
12)	$3^2.5^7.79$	$2^{29}.13$	$11^7.19^2$	4.02943	A. Nitaj
13)	2.5^9	3^{14}	$7^5.11.47$	4.01342	A. Nitaj
14)	$2^{10}.19^{10}$	$5^6.13^4.29^5$	$3^{20}.4425749$	4.00292	A. Nitaj
15)	$5^3.11^4.31^2$	$3^{17}.7^2$	$2^{25}.241$	4.00087	A. Nitaj
16)	$2^8.7^2.19^6$	$5^9.113^2.193$	3.23^9	3.99793	A. Nitaj
17)	$7^7.11^3$	$2^{18}.3^4.103$	$5^9.41^2$	3.99129	A. Nitaj
18)	$2^{10}.7$	5^7	$3^8.13$	3.98092	B.M.M. de Weger
19)	19^8	31^7	$2^{11}.7^4.9049$	3.97796	A. Nitaj
20)	$2^{15}.3.19.29^2$	$5^{10}.7^4$	$13^2.23^6$	3.97457	A. Nitaj
21)	7^9	$3^2.5^7.13^3$	$2^{16}.19^2.67$	3.97414	J. Kanapka
22)	$3^{10}.7^4.11^2$	$17^6.31$	$2^{14}.103^3$	3.96813	A. Nitaj
23)	$2^{13}.47^3$	$3^9.17^3.23$	$7^2.13^7$	3.96555	A. Nitaj
24)	$7^2.17^4.856897$	$2^{41}.3^2$	13^{12}	3.96025	A. Nitaj

Table 4 (continued)

Nr	X	Y	Z	ρ	First author
25)	$2^{25}.3^{4}.29.10753$	$7^{4}.151^{2}.181^{4}$	5^{24}	3.95603	A. Nitaj
26)	61^{4}	$3^{13}.53$	$2^{13}.5.7^{4}$	3.95432	A. Nitaj
27)	$3^{13}.19$	7.53^{4}	$2^{10}.17^{4}$	3.95368	A. Nitaj
28)	$2^{19}.367^{3}$	$5^{17}.197.281$	$13^{2}.251^{6}$	3.94750	A. Nitaj
29)	$2^{11}.17^{4}$	$3^{14}.7^{3}$	$5^{6}.23.71^{2}$	3.94732	A. Nitaj
30)	$2^{9}.37^{3}.89$	$3^{9}.5^{9}.31$	103^{6}	3.94362	A. Nitaj
31)	$7^{5}.23^{2}.41^{4}$	$2^{9}.3^{8}.5^{6}.17^{3}$	$19^{9}.877$	3.93186	A. Nitaj
32)	$11^{8}.13.37$	$3^{5}.5^{7}.23^{3}$	$2.7^{6}.17^{5}$	3.92463	A. Nitaj
33)	7.11^{5}	$3^{9}.17^{2}$	$2^{19}.13$	3.92103	A. Nitaj
34)	$2^{36}.59^{3}$	$11^{2}.13.97^{6}.193$	$3^{8}.5^{7}.19^{2}.113^{3}$	3.91921	A. Nitaj
35)	$3^{8}.227$	$2^{13}.13^{3}$	11^{7}	3.91680	A. Nitaj
36)	$2.7^{4}.53.199^{2}$	$3^{20}.5$	31^{7}	3.91546	A. Nitaj
37)	7^{3}	3^{10}	$2^{11}.29$	3.91498	B.M.M. de Weger
38)	$7^{2}.11^{3}.89.61^{3}$	3^{26}	$2^{6}.5^{12}.13.19$	3.91016	A. Nitaj
39)	$7^{10}.13^{2}.19$	$3^{9}.23.2017^{2}$	$2^{39}.5$	3.90797	A. Nitaj
40)	$3^{8}.17^{4}$	$2^{12}.2917^{2}$	$5^{13}.29$	3.90706	A. Nitaj
41)	$5^{7}.37$	$7^{5}.19^{2}$	$2^{12}.3^{7}$	3.90705	A. Nitaj
42)	$3^{20}.89.647$	$2^{10}.5^{12}.13^{3}$	$7^{3}.11^{8}.101^{2}$	3.90650	A. Nitaj
43)	$2^{25}.5^{3}.17$	$3^{19}.191$	$7^{5}.13^{5}.47$	3.90577	A. Nitaj
44)	$3^{2}.11^{6}$	2^{35}	$19^{5}.13883$	3.90495	B-B
45)	$3^{9}.163$	$2^{3}.11^{6}.17$	5^{12}	3.90458	B-B, A. Nitaj
46)	$2^{6}.7.73^{5}$	13.17^{9}	$3.5^{4}.19.37^{5}$	3.89774	A. Nitaj
47)	2^{21}	$5.11^{4}.17$	$3^{2}.13^{5}$	3.89491	A. Nitaj
48)	$5^{12}.29^{3}$	$13^{2}.19.97^{3}$	$2^{13}.3^{2}.769^{3}$	3.89428	A. Nitaj

Table 4 (continued)

Nr	X	Y	Z	ρ	First author
49)	$7^6.229$	$2^2.5^2.11^5$	3^{16}	3.89124	A. Nitaj
50)	$2^9.3^{10}$	$41^4.73$	$7^2.13^6$	3.88985	A. Nitaj
51)	$7^{13}.11$	$5^6.17^2.23^4$	$2.3^7.37^2.73^3$	3.88786	A. Nitaj
52)	$5^8.14747$	$2^6.3^{17}$	107^5	3.88584	B-B
53)	$2^{14}.5^2.19^2$	3^{18}	$13.17^5.29$	3.88358	A. Nitaj
54)	71.3319^3	$2^{11}.3^2.19^7.601$	17^{13}	3.88214	A. Nitaj
55)	$3^2.5^7.7^9$	$19^6.31^2.149$	$2^{26}.23^3.43$	3.88148	A. Nitaj
56)	$7.17.23^6$	$13^2.109^4$	$2^{15}.3^4.5^6$	3.87332	A. Nitaj
57)	$2^9.11.503^3$	$5^{12}.7^5.13$	$3^{10}.971^3$	3.86720	A. Nitaj
58)	$53^4.139^2$	$2^{21}.11.23^3$	$3^8.5^8.13^2$	3.86707	A. Nitaj
59)	$3^7.5^{12}.11.17$	$2^{35}.23.4969$	$7^4.109^6$	3.86658	A. Nitaj
60)	$5^7.157$	$2^4.19^5$	$3^2.7^8$	3.86443	A. Nitaj
61)	$7^5.11.73^2$	$2^{25}.131$	$3^{16}.5^3$	3.86255	A. Nitaj
62)	$5^{14}.8933$	$2^{23}.13^2.41^3$	$3^{11}.7^4.71^3$	3.86215	A. Nitaj
63)	$11^4.23^6.37^3$	$2^6.19^9.6113$	$3^{10}.5^6.13^6.53$	3.85830	A. Nitaj
64)	$5^7.941^3$	$3^{22}.2503$	$2^{17}.1031^3$	3.85420	A. Nitaj
65)	$3^{22}.71$	$2^2.5^7.23^5$	$7^7.37.373^2$	3.85305	A. Nitaj
66)	$7^2.47^3.151^2$	$5^2.17^{10}$	$2^3.3^{16}.383^2$	3.85206	A. Nitaj
67)	$3^8.5^3.103^2$	$7^9.17^2.37$	$2^4.31^7$	3.85135	A. Nitaj
68)	$3^9.43^3$	$5^{13}.5323$	$2^7.7^3.23^6$	3.85026	A. Nitaj
69)	$2^{13}.7^4.17.29^3$	$3^{20}.31$	$11^3.13^3.41^4$	3.84962	A. Nitaj
70)	$3^9.29$	$7^6.43^2$	$2^{24}.13$	3.84578	A. Nitaj
71)	5^9	$3.11^2.13^4$	$2^{18}.47$	3.84519	A. Nitaj
72)	$2^{33}.5$	$3^9.7^6.31^2.97$	$11^2.19^3.127^4$	3.84392	A. Nitaj

Table 4 (continued)

Nr	X	Y	Z	ρ	First author
73)	$2^{15}.7^4.659$	$23^7.37$	$3^{21}.17$	3.84365	A. Nitaj
74)	3.29^7	$5^8.11^4.17$	$2^5.31^4.71^2$	3.84322	A. Nitaj
75)	3.7^{17}	$2^{14}.41^3.547^3$	$11.13^9.29^2.31.61$	3.83721	A. Nitaj
76)	$5^{14}.7^6$	$2^{33}.3.17.5471$	$41^4.1033^3$	3.83711	A. Nitaj
77)	2^{17}	$5^5.71$	3.7^6	3.83645	A. Nitaj
78)	$109^3.2383^3$	$2^{50}.7^2.17.19.31$	$3^{17}.53^6.193$	3.83622	A. Nitaj
79)	$11^5.191^3$	$3^6.5^8.7^3.29^2$	$2^2.13^{10}.151$	3.83512	A. Nitaj
80)	$7^5.17^4$	$2^2.3.5.31^6$	$13^8.67$	3.83405	A. Nitaj
81)	$3^4.11^8.59.89$	$7^{12}.47^2.173$	$2^{21}.37^6$	3.82814	A. Nitaj
82)	$5^5.17.43^2.59$	$2^{31}.11$	$3^6.7^9$	3.82640	A. Nitaj
83)	23.701^4	$2.11^6.13.17^5$	$3.5^{17}.31$	3.82619	A. Nitaj
84)	$5^4.17^6$	$3^{13}.23^2.101$	$2^{15}.11^5.19$	3.82547	A. Nitaj
85)	$19^9.4978973$	$7^{13}.367^3$	$2^4.3^6.11^5.23^7$	3.82319	A. Nitaj
86)	$17^9.61861.77279$	$7^{10}.373^5$	$2^{17}.5^{16}.19^4$	3.82278	A. Nitaj
87)	2^{17}	$3^{10}.17$	5.61^3	3.82250	A. Nitaj
88)	$3^{13}.5^4.23.73^3$	$2^{24}.13^{12}$	$11^{12}.29.4294769$	3.82096	A. Nitaj
89)	17^7	$13^6.103$	$2^5.3.5^7.11^2$	3.82031	A. Nitaj
90)	7^{11}	$2^4.3^{15}.11$	$5^8.11527$	3.81827	A. Nitaj
91)	$2^7.5^2.7^2.103^3$	$3^{12}.11^6.19$	$13^{10}.131$	3.81767	A. Nitaj
92)*	$3^3.47^2.2081$	2^{37}	5.31^7	3.81593	B-B
93)	$3^6.11^4.23^3.37^2$	$2^{11}.61^6$	$5^{15}.9283$	3.81427	A. Nitaj
94)	$3^{13}.37.79$	$2^{18}.5^5.7^2$	$11^9.19$	3.81383	A. Nitaj
95)	$5^9.23$	$2^6.3^5.17^3$	$7^2.19^5$	3.81382	A. Nitaj
96)	$2^{27}.11$	$5^9.853$	$3^{16}.73$	3.81361	A. Nitaj

Table 4 (continued)

Nr	X	Y	Z	ρ	First author
97)*	$2^{12}.13^2.271$	$3^{10}.11.53^3$	7^{13}	3.81119	B-B
98)	$3^8.56599^2$	$13^4.23^5.37^2$	$2^{43}.31$	3.80972	A. Nitaj
99)*	$7^3.103.2887403261$	$2^7.5^{25}$	$3^{25}.19^6$	3.80887	B-B
100)	$2^6.5.137$	3^{14}	13^6	3.80839	B-B, A. Nitaj
101)	$2^5.3^{18}$	$5^6.7^{10}.23^2$	$11^9.990203$	3.80838	A. Nitaj
102)	19^5	$2^{12}.11^3$	$3^7.5^3.29$	3.80812	A. Nitaj
103)	$3^{15}.7$	$2^7.23.59^3$	$5^9.19^2$	3.80656	A. Nitaj
104)	149^4	$2^5.5^5.7^2.13.47$	3^{20}	3.80576	A. Nitaj
105)	$2^{26}.41^2$	$7^3.1217^3$	$3^{19}.17.37$	3.80565	A. Nitaj
106)*	$2^6.7^3.17.29.503$	11^{10}	3^{22}	3.80274	B-B

APPENDICES

Appendice A: Les courbes elliptiques

Appendice B: Les fractions continues

Appendice C: Résolution des congruences

Appendice A

Les courbes elliptiques

1. Généralités

La théorie des courbes elliptiques est vaste. Dans cet appendice, nous nous bornerons à quelques définitions et propriétés dont nous avons besoin sur les courbes elliptiques définies sur $\mathbb{Q}$. Pour plus amples informations, voir par exemple [Sil1].
Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (a_i \in \mathbb{Q}). \tag{1}$$

Suivant [Sil1], on définit les quantités:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= a_1a_3 + 2a_4,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6.
\end{aligned}$$

Le discriminant de E sur $\mathbb{Q}$ est:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0.$$

L'invariant absolu de E est:

$$j = \frac{c_4^3}{\Delta}.$$

Il existe plusieurs relations entre les quantités associées à une courbe elliptique. En particulier, nous avons les suivantes:

$$\begin{aligned}
4b_8 &= b_2b_6 - b_4^2,\\
1728\Delta &= c_4^3 - c_6^2.
\end{aligned}$$

A un isomorphisme près, la courbe elliptique E est définie sur $\mathbb{Q}$ par son invariant absolu j. Tout isomorphisme préservant la forme de Weierstrass de E sur $\mathbb{Q}$ est une transformation du type:

$$\begin{aligned}
x &= u^2x' + r,\\
y &= u^3y' + u^2sx' + t,
\end{aligned}$$

avec u, r, s, t rationnels et $u \neq 0$. Cet isomorphisme transforme la courbe eeliptique E définie par l'équation (1) en une courbe elliptique E' définie sur $\mathbb{Q}$ par l'équation:

$$E' : {y'}^2 + a'_1 x' y' + a'_3 y' = {x'}^3 + a'_2 {x'}^2 + a'_4 x' + a'_6, \qquad (a'_i \in \mathbb{Q}),$$

pour laquelle on a:

$$c'_4 = u^{-4} c_4,$$
$$c'_6 = u^{-6} c_6,$$

et le discriminant:

$$\Delta' = u^{-12} \Delta.$$

L'invariant absolu reste le même. On peut alors simplifier l'équation (1) en remplaçant y par $(y - a_1 x - a_3)/2$, ce qui donne une nouvelle équation pour E:

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6. \tag{2}$$

On peut aussi simplifier l'équation ci dessus en remplaçant x par $(x - 3b_2)/36$ et y par $y/216$, ce qui donne une nouvelle équation pour E:

$$E : y^2 = x^3 - 27c_4 x - 54c_6.$$

On vient de montrer que toute courbe elliptique définie sur $\mathbb{Q}$ peut se mettre sous une forme de Weierstrass courte:

$$E : y^2 = x^3 + Ax + B, \qquad (A, B \in \mathbb{Q}),$$

ayant pour discriminant:

$$\Delta = -16(4A^3 + 27B^2),$$

et pour invariant absolu:

$$j = 1728 \frac{(4A)^3}{\Delta}.$$

2. Modèle minimal d'une équation de Weierstrass

Soit p un nombre premier. Pour tout nombre rationnnel $r = \frac{m}{n} p^{\nu}$, avec m et n premier avec p, on pose:

$$\mathrm{ord}_p(r) = \nu,$$

et par convention $\mathrm{ord}_p(0) = \infty$. On peut définir alors une valeur absolue non-archimédienne $|.|_p$ en posant pour tout rationnel r:

$$|r|_p = p^{-ord_p(r)},$$

et, toujours par convention, $|0|_p = 0$. Cette valeur absolue est appelée valeur absolue p-adique sur $\mathbb{Q}$.
Soit E une courbe elliptique définie par l'équation de Weierstrass (1). Soit d le dénominateur commun des a_i. En remplaçant x par $d^{-2}x$ et y par $d^{-3}y$, on obtient une équation de Weierstrass dont tous les a_i sont entiers. Alors le discriminant Δ est entier, et pour tout nombre premier p, on a $\mathrm{ord}_p(\Delta) \geq 0$. On pose alors la définition suivante:

Définition 1. *Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation de Weierstrass (1). Cette équation est dite minimale si chaque a_i est entier et si pour tout nombre premier p, $ord_p(\Delta)$ est minimal. Le discrminant minimal de la courbe elliptique E est alors Δ.*

En pratique, pour reconnaître un modèle minimal, il faut considérer les quantités c_4 (ou c_6) et Δ. On sait que toute courbe elliptique E définie sur $\mathbb{Q}$ admet une équation de Weierstrass courte:

$$E : y^2 = x^3 - 27c_4x - 54c_6, \qquad (c_4, c_6 \in \mathbb{Z}),$$

de discriminant Δ. Si p est un nombre premier tel que $p^4|c_4$ et $p^{12}|\Delta$, alors en remplaçant x par p^2x et y par p^3y, on obtient une nouvelle équation:

$$E : y^2 = x^3 - 27c_4'x - 54c_6' \qquad (c_4', c_6' \in \mathbb{Z}),$$

avec $c_4' = p^{-4}c_4$ et $c_6' = p^{-6}c_6$, et de discriminant $\Delta' = p^{-12}\Delta$. On peut continuer ainsi cette descente en considérant tous les facteurs premiers de (c_4, Δ). Une équation de Weierstrass à coefficient dans $\mathbb{Z}$ est un modèle minimal si pour tout nombre premier p, on a l'une ou l'autre des conditions:

$$\mathrm{ord}_p(\Delta) < 12 \quad \text{ou} \quad \mathrm{ord}_p(c_4) < 4.$$

3. Courbes elliptiques semi-stables. Conducteur

Définition 2. *Soit E une courbe elliptique définie sur $\mathbb{Q}$ par un modèle minimal de Weierstrass:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (a_i \in \mathbb{Z}).$$

Soit p un nombre premier.
- E a bonne réduction en p si $ord_p(\Delta) = 0$.
- E a mauvaise réduction de type multiplicatif en p si $ord_p(\Delta) > 0$ et $ord_p(c_4) = 0$.

- *E a mauvaise réduction de type additif en p si $ord_p(\Delta) > 0$ et $ord_p(c_4) > 0$.*
- *E est dite semi-stable en p si elle a bonne réduction ou mauvaise réduction de type multiplicatif en p.*

On déduit donc, d'après cette définition, les propriétés suivantes:
- Une courbe elliptique est stable en tout nombre premier ne divisant pas son discriminant minimal.
- Une courbe elliptique non stable en un nombre premier p est semi-stable en p si les quantités c_4 et Δ de son modèle minimal sont telles que $|c_4, \Delta|_p = 1$.
- Une courbe elliptique non stable en un nombre premier p est instable en p si les quantités c_4 et Δ de son modèle minimal sont tels que $|(c_4, \Delta)|_p < 1$.

Nous donnons maintenant la définition d'une courbe elliptique semi-stable.

Définition 3. *Une courbe elliptique semi-stable en tout nombre premier est dite semi-stable.*

On peut maintenant donner la définition du conducteur d'une courbe elliptique.

Définition 4. *Soit E une courbe elliptique définie sur $\mathbb{Q}$, de discriminant minimal Δ_E. Le conducteur de E est défini par:*

$$N_E = \prod_{p|\Delta_E} p^{m_p},$$

avec

$$m_p = \begin{cases} 1 \text{ si la courbe est semi-stable en } p, \\ 2 \text{ si la courbe est instable en } p \text{ et si } p \neq 2,3, \\ 2+\varepsilon_p \text{ si la courbe est instable en } p = 2,3, \text{ avec } 0 \leq \varepsilon_p \leq 7. \end{cases}$$

Pour une définition plus détaillée, et pour une signification exacte de ε_p, on peut consulter par exemple [Sil1], p.361

D'après cette définition, on remarque que si E est une courbe elliptique semi-stable, alors son conducteur est le produit des facteurs premiers divisant son discriminant:

$$N_E = \prod_{p|\Delta_E} p = r(\Delta_E).$$

Appendice B

Les fractions continues

Dans cet appendice, on rappelle quelques résultats généraux et classiques sur le développement en fraction continue d'un réel. On se limitera cependant aux besoins de cette thèse. Les démonstration de tous les résultats cités dans cet appendice se trouvent dans la plupart des livres de Théorie des Nombres, comme par exemples dans [Ni-Zu-Mo]. La fraction continue d'un nombre réel ξ s'obtient de la façon suivante. On écrit:

$$\xi = a_0 + \frac{1}{\xi_1},$$

où $a_0 = [\xi]$ est la partie entière de ξ. On recommence ensuite en remplaçant dans l'expression ci dessus ξ par ξ_1, ce qui donne un entier a_1 et un réel ξ_2. On obtient ainsi les formules de récurrence:

$$\xi_i = a_i + \frac{1}{\xi_{i+1}}, \qquad i \geq 0,$$

avec $\xi_0 = \xi$ et $a_i = [\xi_i]$. On a alors l'expression:

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}},$$

et on écrit tout simplement $\xi = [a_0, a_1, a_2, a_3, \cdots]$, qu'on appelle développement de ξ en fraction continue. Si ξ est rationnel, son développement en fraction continue est fini. En odoptant la convention que le dernier terme, s'il existe, est strictement supérieur à 1, alors le développement en fraction continue de tout réel est unique. Pour $i \geq 0$, les réduites $\frac{u_i}{v_i}$ de ξ sont obtenues en prenant $(u_i, v_i) = 1$ et

$$\frac{u_i}{v_i} = [a_0, \cdots, a_i].$$

Si on convient que $u_{-2} = 0, v_{-2} = 1, u_{-1} = 1, v_{-1} = 0$, alors on a les relations de récurrence:

$$u_i = a_i u_{i-1} + u_{i-2},$$
$$v_i = a_i v_{i-1} + v_{i-2},$$

pour tout $i \geq 0$.

Comme principales propriétés des réduites, nous avons:

$$u_i v_{i-1} - u_{i-1} v_i = (-1)^{i-1}, \qquad i \geq 1,$$
$$u_i v_{i-2} - u_{i-2} v_i = (-1)^i a_i, \qquad i \geq 1,$$
$$\left|\xi - \frac{u_i}{v_i}\right| < \frac{1}{v_i v_{i+1}} \leq \frac{1}{v_i^2}, \qquad i \geq 0.$$

Si d est un entier positif, non carré parfait, alors son développement en fraction continue est périodique et:

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0}],$$

où $a_0 = \left[\sqrt{d}\right]$. Sa période est alors la suite $(a_1, a_2, \cdots, a_{r-1}, 2a_0)$, de longeur r. Si le développement du réel non nul ξ est $\xi = [a_0, a_1, a_2, a_3, \cdots]$, alors, les développements en fraction continue de $-\xi$ et de $1/\xi$ s'obtiennent à l'aide des formules

$$-\xi = \begin{cases} [-a_0 - 1, 1, a_1 - 1, a_2, a_3, \cdots], & \text{si } a_1 > 1, \\ [-a_0 - 1, a_2 + 1, a_3, \cdots], & \text{si } a_1 = 1, \end{cases}$$
$$\frac{1}{\xi} = \begin{cases} [0, a_0, a_1, a_2, \cdots], & \text{si } \xi > 1, \\ [a_1, a_2, a_3, \cdots], & \text{si } 0 < \xi < 1. \end{cases}$$

Nous allons maintenant énoncer un théorème (sans démonstration).

Théorème 1. *Soit ξ un nombre réel non nul. Soient $\frac{u_n}{v_n}$ et $\frac{u_{n+1}}{v_{n+1}}$ deux réduites consécutives de ξ. Pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $b < v_{n+1}$, alors $|b\xi - a| \geq |v_n \xi - u_n|$.*

Une preuve de ce théorème se trouve dans les références citées au début de cet appendice. Le seul résultat que nous allons montrer concernant les fractions continues est le théorème suivant (il servira assez souvent dans cette thèse).

Théorème 2. *Soit ξ un nombre réel. Si la fraction irréductible $\frac{a}{b}$ avec $b \geq 1$ vérifie:*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

alors $\frac{a}{b}$ est une réduite de la fraction continue de ξ.

Preuve. Si $\xi = \frac{a}{b}$, le théorème est trivial. Si $b = 1$, alors $|\xi - a| < \frac{1}{2}$, et donc $a = [\xi]$ ou $a = [\xi] + 1$. Dans les deux cas $\frac{a}{1}$ est une réduite de ξ et le théorème est vérifié. Supposons maintenant que $b > 1$ et que $\xi \neq \frac{a}{b}$. Soit n un entier vérifiant $v_n \leq b < v_{n+1}$. D'après le théorème 1, on a $|v_n \xi - u_n| \leq |b\xi - a| < \frac{1}{2b}$. Supposons que $\frac{a}{b} \neq \frac{u_n}{v_n}$. Alors on a:

$$\frac{1}{bv_n} \leq \frac{|bu_n - av_n|}{bv_n} = \left|\frac{u_n}{v_n} - \frac{a}{b}\right| \leq \left|\xi - \frac{u_n}{v_n}\right| + \left|\xi - \frac{a}{b}\right| < \frac{1}{2bv_n} + \frac{1}{2b^2} = \frac{b + v_n}{2b^2 v_n},$$

d'où $b < v_n$, ce qui contredit la définition de n.

Appendice C

Résolution des congruences

Nous aurons souvent besoin de résoudre des congruences, en particulier des congruences du type:

$$x^n \equiv a \pmod{m},$$

où a et m sont des entiers premiers entre eux. Résoudre de telles congruences peut s'avérer un problème difficile lorsque m est assez grand. Très peu de méthodes sont connues pour les traiter. Pour celles qu'on va décrire dans cet appendice, nous supposons que la factorisation de m est donnée sous la forme $m = p_1^{e_1} \dots p_r^{e_r}$. Le théorème des restes chinois permet d'isoler r congruences sous la forme:

$$x^n \equiv a \pmod{p^e} \tag{1.}$$

où p décrit l'ensemble des nombre premiers divisant m avec pour multiplicité e. Pour le nombre de solutions de la congruence (1) lorsque $p \geq 3$, nous avons le théorème suivant:

Théorème 1. *Soit p un nombre premier impair. Soit a un entier premier avec p. La congruence (1) admet $k = (n, p^{e-1}(p-1))$ solutions si*

$$a^{p^{e-1}(p-1)/k} \equiv 1 \pmod{p^e},$$

et aucune solution sinon.

Preuve. Soit g un générateur du groupe des unités de $\mathbb{Z}/p^e\mathbb{Z}$. Puisque $(a,p) = 1$, alors $a = g^i$ pour un entier i. Si la congruence (1) a une solution x, alors $(x,p) = 1$ et donc $x = g^y$ pour un certain entier y. La congruence est alors équivalente à la nouvelle congruence:

$$ny \equiv i \pmod{p^{e-1}(p-1)}. \tag{2}$$

Soit $k = (n, p^{e-1}(p-1)$. Posons $n' = n/k$. Si $k|i$, alors $i = ki'$ et la congruence (2) devient:

$$n'y \equiv i' \pmod{p^{e-1}(p-1)/k},$$

ce qui donne k solutions $y = i'n'^{-1} + jp^{e-1}(p-1)/k$, $j = 0, 1, \cdots k-1$ où n'^{-1} est un inverse de n' modulo $p^{e-1}(p-1)/k$. Ainsi la congruence (1) a dans ce cas k solutions et on a:

$$a^{p^{e-1}(p-1)/k} \equiv g^{ip^{e-1}(p-1)/k} \equiv 1 \pmod{p^e},$$

puisque $ip^{e-1}(p-1)/k \equiv 0 \pmod{p^{e-1}(p-1)}$. Si $k \not| i$, alors la congruence (2) n'a pas de solution et dans ce cas, on a:

$$a^{p^{e-1}(p-1)/k} \equiv g^{ip^{e-1}(p-1)/k} \not\equiv 1 \pmod{p^e},$$

puisque $ip^{e-1}(p-1)/k \not\equiv 0 \pmod{p^{e-1}(p-1)}$. ∎

Posons maintenant $n = p^\beta n'$ avec $(p, n') = 1$. On a alors:

$$\left(n, p^{e-1}(p-1)\right) = \left(p^\beta n', p^{e-1}(p-1)\right) = \left(p^\beta, p^{e-1}\right)(n', p-1).$$

Si $e > \beta$, la résolution de la congruence (1) peut se faire en deux étapes: Résoudre la congruence

$$t^{p^\beta n'} \equiv a \pmod{p^{\beta+1}},$$

puis en utilisant le lemme de Hensel et la méthode de Newton, on peut remonter jusqu'aux solutions de la congruence (1). Ceci est utilisé plus en détail dans le chapitre 3, partie III. Quand au nombre de solutions de la congruence (1) lorsque $p = 2$, il est déterminé par le théorème suivant:

Théorème 2. *Soit a un entier impair et $p = 2$. Si $e = 0$ ou $e = 1$ ou si $e \geq 2$ et n impair, la congruence (1) admet une solution. Si $e \geq 2$ et n est pair, elle admet $2(n, 2^{e-2})$ solutions si $a \equiv 1 \pmod{4(n, 2^{e-1})}$ et aucune solution sinon.*

Preuve. La preuve se base sur l'ordre de 5 modulo 2^e (voir [Ni-Zu-Mo], p.105). ∎

Dans le cas $p = 2$, posons $n = 2^\beta n'$ où n' est impair et β positif. Si $e > \beta + 2$, alors la congruence (1) peut être résolue aussi en deux étapes: résoudre la congruence

$$t^n \equiv a \pmod{2^{\beta+2}},$$

puis en utilisant le lemme de Hensel et la méthode de Newton, remonter jusqu'aux solutions de la congruence (1). ∎

Nous aurons souvent affaire à la congrunce suivante:

$$x^2 \equiv a \pmod{p}, \tag{3}$$

où a est un entier et p un nombre premier impair avec $(a, p) = 1$. Cette congruence, d'après le théorème 1 admet 2 solutions si $a^{(p-1)/2} \equiv 1 \pmod p$ ou aucune solution sinon. On peut donc dire qu'elle admet $1 + \left(\dfrac{a}{p}\right)$ solution où $\left(\dfrac{a}{p}\right)$ désigne le symbole de

Legendre. Nous allons décrire maintenant un algorithme pour résoudre la congruence (3). Cet algorithme s'appelle Ressol et est dû à D. Shanks (voir [Ni-Zu-Mo]).

Algorithm Ressol

Entrée: a, p premier.

Calculer le symbole de Legendre $s := \left(\dfrac{a}{p}\right)$.

> **Si** $s = -1$, il n'y a pas de solution: **stop**;
>
> **Sinon**
>
> > **Si** $p \equiv 3 \pmod 4$, $x := \pm a^{(p+1)/4}$ est solution: **stop**;
> >
> > Déterminer $k_0 \geq 2$ et m impair tels que $p - 1 = 2^{k_0} m$;
> >
> > $r_0 :\equiv a^{(m+1)/2} \pmod p$;
> >
> > $n_0 :\equiv a^m \pmod p$;
> >
> > **Si** $n_0 \equiv 1 \pmod p$, $x := \pm r_0$ est solution: stop
> >
> > **Sinon**
> >
> > > Déterminer un non-résidu quadratique z modulo p;
> > >
> > > $c_0 :\equiv z^m \pmod p$;
> > >
> > > $i := 0$;
> > >
> > > **Tant que** $n_i \not\equiv 1 \pmod p$ **répéter**
> > >
> > > > Déterminer l'ordre $2^{k_{i+1}}$ de n_i;
> > > >
> > > > $b_{i+1} :\equiv c_i^{2^{k_i - k_{i+1} - 1}} \pmod p$;
> > > >
> > > > $r_{i+1} :\equiv b_{i+1} r_i \pmod p$;
> > > >
> > > > $c_{i+1} :\equiv b_{i+1}^2 \pmod p$;
> > > >
> > > > $n_{i+1} :\equiv c_{i+1} n_i \pmod p$;
> > > >
> > > > **Si** $n_{i+1} \equiv 1 \pmod p$, $x := \pm r_{i+1}$ est solution: **stop**;
> > > >
> > > > **Sinon** $i := i + 1$;

Sortie: Solutions de la congruence $x^2 \equiv a \pmod p$.

Nous donnons maintenant la démonstration de cet algorithme ainsi qu'une estimation de sa complexité.

Théorème 3. *L'algorithme Ressol termine toujours, avec une complexité en*

$$O\left(p^{(4\sqrt{e})^{-1} + \varepsilon}\right),$$

où e désigne ici la base de l'exponentielle et où ε est une constante positive indépendante de p et de a.

Preuve. Soit $s = \left(\dfrac{a}{p}\right)$. Si $s = -1$, alors a n'est pas un résidu quadratique modulo p et donc la congruence (3) n'a pas de solutions. Supposons que $s = 1$.
Si $p \equiv 3 \pmod 4$, alors:

$$\left(\pm a^{(p+1)/4}\right)^2 = a^{(p+1)/2} = aa^{(p-1)/2} \equiv a \pmod p,$$

ce qui donne les deux solutions de la congruence (3).
Supposons maintenant que $p \equiv 1 \pmod 4$. Ecrivons $p - 1 = 2^{k_0}m$ avec $k_0 \geq 2$ et m impair. Des expressions de r_0 et n_0, on obtient:

$$r_0^2 \equiv an_0 \pmod p,$$

et donc si $n_0 \equiv 1 \pmod p$, alors $\pm r_0$ sont les solutions de la congruence (3). La détermination d'un non-résidu quadratique z modulo p se fait en:

$$O\left(p^{\left(4\sqrt{e}\right)^{-1}+\varepsilon}\right),$$

où ε est une constante absolue. En pratique, z peut être déterminé en testant les premiers entiers. Soit $c_0 \equiv z^m \pmod p$. On a alors:

$$c_0^{2^{k_0-1}} \equiv z^{2^{k_0-1}m} \equiv z^{(p-1)/2} \equiv -1 \pmod p.$$

Ainsi l'ordre de c_0 est 2^{k_0}.
D'autre part, si $n_0 \not\equiv 1 \pmod p$, alors:

$$n_0^{2^{k_0-1}} \equiv a^{2^{k_0-1}m} \equiv a^{(p-1)/2} \equiv 1 \pmod p,$$

puisque a est un résidu quadratique modulo p. Ceci signifie que l'ordre de n_0 est de la forme 2^{k_1} avec $k_1 < k_0$.
En multipliant la congruence $r_0^2 \equiv an_0 \pmod p$ par b_1^2, on obtient $b_1^2 r_0^2 \equiv ab_1^2 n_0 \pmod p$ et donc:

$$r_1^2 \equiv an_1 \pmod p.$$

Si $n_1 \equiv 1 \pmod p$, alors d'après la congruence ci dessus, on a $r_1^2 \equiv a \pmod p$ et donc $x = \pm r_1 \pmod p$. Si ce n'est pas le cas, on doit recommencer le procédé où cette fois c_1 sera d'ordre 2^{k_1} avec $k_1 < k_0$.
Cet algorithme termine car la suite (k_i) est strictement décroissante. ∎

Remarque. Si un non-résidu quadratique modulo p est donné, la complexité de l'algorithme est seulement en $O(\log p)$.

On considère maintenant la congruence:

$$x^q \equiv a \pmod p,$$

où p et q sont des nombres premiers impairs. Nous donnons, sans démonstration l'algorithme ci-dessous pour résoudre cette congruence. La version détaillée se trouve dans [Wil-Har].

Algorithme de résolution de la congruence $x^q \equiv a \pmod p$

Entrée: Deux nombres premiers impairs p et q et un entier non nul a.

Si $p = q$ **alors** $x :\equiv a \pmod p$ est solution; **Stop**;
Sinon
  Si $p \not\equiv 1 \pmod q$ **alors**
    calculer $u :\equiv q^{-1} \pmod{p-1}$, $0 < u < p-1$,
    $x :\equiv a^u \pmod p$ est solution; **Stop**
  Sinon
    Calculer $s \equiv a^{(p-1)/q} \pmod p$;
    Si $s \neq 1$ **alors** pas de solution; **Stop**
    Sinon
      $b := 1$;
      Tant que $(b^q - a)^{(p-1)/q} \equiv 0, 1 \pmod p$ **faire** $b := b + 1$;
      $c :\equiv (b^q - a)^{(p-1)/q} \pmod p$;
      $\theta := (b^q - a)^{1/q}$;
      $Base := (1, \theta, \theta^2, \cdots, \theta^{q-1})$;
      Pour $i = 0$ **à** $q - 2$ calculer dans $Base$

$$X_i := (b - c^i\theta)^{(-1)^{q-i}\binom{q-1}{i}};$$

      Pour $i = 1$ **à** $q - 1$ calculer dans $Base$

$$Y_i := (b - c^{q-i-1}\theta)^{\left(1-(-1)^i\binom{q-1}{i}\right)/q};$$

      Calculer

$$E_1 := \prod_{i=0}^{q-2} X_i = \sum_{i=0}^{q-1} a_i\theta^i, \quad 0 \leq a_i \leq p-1;$$

$$E_2 := \prod_{i=1}^{q-1} Y_i = \sum_{i=0}^{q-1} b_i\theta^i, \quad 0 \leq b_i \leq p-1;$$

Pour $i = 0$ **à** $q-1$ **faire**

$a_i(1) := a_i;$

Calculer $a_i((p-1)/q)$ en utilisant la formule de récurrence:

$$a_i(m+n) := \sum_{j=0}^{i} a_j(m)a_{i-j}(n) + (b^q - a)\sum_{j=i+1}^{q-1} a_j(m)a_{q+i-j}(n), \quad m, n = 1, 2, \cdots;$$

Calculer

$$x^{(0)} := a_0((p-1)/q)b_0 + (b^q - a)\sum_{i=1}^{q-1} a_i((p-1)/q)b_{q-i};$$

Pour $j = 1$ **à** $q-1$ calculer $x^{(j)} := c^j x^{(0)};$

Sortie: Les solutions $x^{(j)}$, $0 \leq j \leq q-1$ de la congruence $x^q \equiv a \pmod{p}$. ■

La complexité de l'algorithme ci-dessus est en (voir [Wil-Har]):

$$O\left(q^4\right) + O\left(q^2 \log(p)\right).$$

Bibliographie

[Bac] G. Bachmann, *Introduction to p-adic Numbers and Valuation Theory,* Academic Press, New York and London, 1964.

[Bak] A. Baker, *Bounds for the solutions of the hyperelliptic equation,* Proc. Camb. Phil. Soc. **65** (1969), 439 – 444.

[Bro-Brz] J. Browkin and J. Brzezinski, *Some remarks on abc-conjecture,* preprint, Université de Göteborg, 1992, à paraître.

[Coh1] J. H. E. Cohn, *The diophatine equation* $x^2 + 19 = y^n$, Acta Arith. **39** (1964), 1537 – 540.

[Coh2] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc. **61** (1992), 193 – 197.

[Cor] G. Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$, Giornale di Matematiche di Battaglini **46** (1908), 33–90.

[Elk] N. D. Elkies, *ABC implies Mordell,* Intern. Math. Res. Notices **7** (1991), 99 – 109.

[Erd-Sho] P. Erdös and T. N. Shorey, *On the greatest prime factor of* $2^p - 1$ *for a prime* p *and other expressions,* Acta Arith. **30** (1976), 257 – 265.

[Eve] J. H. Evertse, *On the equation* $ax^n - by^n = c$, Compositio Math. **47** (1982), 289 – 315.

[Fai] A. Faisant, *L'équation Diophantienne du Second Degré,* Hermann, Paris (1991).

[Fo-Na-Te] E. Fouvry, M. Nair et G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro,* Bull. Soc. Math. France **120** 1992, 485 – 506.

[Fre] G. Frey, *Links between elliptic curves and solutions of* $A - B = C$, Indian Math. Soc. **51** (1987), 117 – 145.

[Guy] R. K. Guy, *Unsolved Problems in Number Theory*, Springer Verlag, 1981.

[Hal] M. Hall Jr, *The diophantine equation* $x^3 - y^2 = k$, Computers in Number Theory, Proceeding of the Science Research Concil Atlas Symposium No. 2, Oxford 1969, Academic Press, London (1971), 173 – 198.

[Ha-Mu-Wi] 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** (1990), $327-343$.

[Hel1] Y. Hellegouarch, *Courbes elliptiques et équation de Fermat,* Thèse (1972), Université de Besançon.

[Hel2] Y. Hellegouarch, *Points d'ordre $2p^h$ sur les courbes elliptiques,* Acta Arith. **26**, (1975), $253-263$.

[Hua] L. K. Hua, *On the least solution of Pell's equation*, Bull. Amer. Math. Soc. **48** (1942), $731-735$.

[Ink] K. Inkeri, *On the diophantine equation $a(ax^n-1)/(x-1) = y^m$,* Acta Arith. **21** (1972), $299-311$.

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

[Lange1] M. Langevin, *Partie sans facteur carré d'un produit d'entiers voisins* , Approximations Diophantiennes et Nombres Transcendants, Luminy 1990, Walter de Druyter and Co. Berlin-New York 1992.

[Lange2] M. Langevin, *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)*, C. R. Acad. Sci. Paris, t. 317 (1993), $441-444$.

[Le1] Le Maohua, *On the diophantine equation $x^2+d=4p^n$*, J. Number Theory. **41** (1992), $87-97$.

[Le2] Le Maohua, *On the diophantine equations $d_1x^2+2^{2m}d_2=y^n$ and $d_1x^2+d_2=4y^n$*, Proc. Amer. Math. Soc. **1** (1993), $67-70$.

[L-L-M-P] A. K. Lernstra, H. W. Lenstra Jr, M. S. Manasse and J. M. Pollard, *The number field sieve,*, Proceedings of AMS-STOC'90, 564-572.

[Lju] W. Ljunggren, *Zur Theorie der Gleichung $x^2+1=dy^4$*,Avh. Norske Vid. Akad. Oslo **5** (1942), $1-27$.

[Mas] R. C. Mason, *Diophantine equations over Function Fields,* LMS Lecture Notes **96**, Cambridge University Press 1984.

[Mon] P. L. Montgomery, *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$,* Math. Comp. **61** (1993), $361-363$.

[Mor] F. Morain, *Courbes elliptiques et tests de primalité,* Thèse (1990), Université de Lyon 1.

[Mord] L. J. Mordell, *Diophantine Equations,* Academic Press (New York), 1969.

[Nit1] A. Nitaj, *Algorithms for finding abc-examples,* preprint n^o 60 (1992), Université de Caen.

[Nit2] A. Nitaj, *Algorithms for finding good examples for the abc and the Szpiro conjectures*, preprint n^o 61 (1993), Université de Caen, à paraître dans *Experimental Mathematics.*

[Nit3] A. Nitaj, *An algorithm for finding good abc-examples*, C. R. Acad. Sci. Paris, t. 317 (1993), 811 – 815.

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

[Oes] 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.

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

[Pil] S. S. Pillai, *On the inequality* $0 < a^x - b^y \leq n$, J. Indian Math. Soc. **37** (1931), 1 – 11.

[Rib1] P. Ribenboim, 13 *Lectures on Fermat's Last Theorem,* Springer-Verlag, 1979.

[Rib2] P. Ribenboim, *Remarks on exponential congruences and powerful numbers,* J. Number Theory, **29** (1988), 251 – 263.

[Rib3] P. Ribenboim, *The Little Book of Big Primes,* Springer-Verlag, 1991.

[Ric] 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 Ser. (C-265), Kluwer, (1989), 529 – 545.

[Rie] H. Riesel, *Prime Numbers and Computer Methods for Factorization,* Birkhäuser, Basel and New York, 1985.

[Ros] K. H. Rosen, *Elementary Number Theory and Its Application*, Addison-Wesley 3rd ed. 1992.

[Sch-Tij] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), 199 – 204.

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

[Sco] R. Scott, *On the diophantine equations $p^x - b^y = c$ and $a^x + b^y = c^z$*, J. Number Theory **44** (1993), $153 - 165$.

[Sho] T. N. Shorey, *On the greatest prime factor of $(ax^m + by^n)$*, Acta Arith. **36** (1980), $21 - 25$.

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

[Sil1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[Sil2] J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226-237.

[Sil3] J. H. Silverman, *Taxicabs and sums of two cubes*, Amer. Math. Monthly **100** (1993), $331 - 340$.

[Sil-Tat] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves,* Springer-Verlag, 1992.

[Sta] H. M. Stark, *Effective estimates of solutions of some diophantine equations,* Acta Arith. **24** (1973), $251 - 259$.

[Ste] C. L. Stewart, *The greatest prime factor of $a^n - b^n$*, Acta Arith. **26** (1975), $427 - 433$.

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

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

[Sto1] C. Stormer, *Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications,* Vid. Skr. I Math. Natur. Kl. (Christiana) 1897 No. 2, **48**, $3-48$.

[Sto2] C. Stormer, *L'équation $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\pi/4$,* Bull. Soc. Math. France **27** (1899), $160 - 170$.

[Szp] L. Szpiro, *Discriminant et conducteur des courbes elliptiques,* Astérisques **183** (1990), $7 - 18$.

[Ter] N. Terai, *The diophantine equation $x^2 + q^m = p^n$,* Acta Arith. **63** (1993), $351 - 358$.

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

[Tza-Wol] N. Tzanakis and J. Wolfskill *On the diophantine equation* $y^2 = 4q^n + 4q + 1$, J. Number Theory. **23** (1986), 219 – 237.

[Va-Gi-To] B. Vallée, M. Girault et P. Toffin, *How to guess l-th roots modulo n by reducing lattice bases*, Comptes Rendus du Congrès AAECC-88, Rome 1988, Lectures Notes in Computer Science (357), 427 – 442.

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

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

[Wil-Har] K. S. Williams and K. Hardy, *A refinement of H. C. Williams'qth root algorithm,* Math. Comp. **61** (1993), 475 – 483.

[Zhe] C. Zhenfu, *On the diophantine equation* $x^{2n} - dy^2 = 1$, Proc. Amer. Math. Soc. **98** (1986), 11 – 16.

RÉSUMÉ: Nous étudions dans cette thèse les conséquences et les aspects expérimentaux de la conjecture *abc* et des conjectures de Szpiro. Nous montrons d'abord comment appliquer ces conjectures pour apporter une réponse à plusieurs conjectures et problèmes ouverts, montrant ainsi leur importance en théorie des nombres. Indépendamment de ces conjectures, nous donnons une démonstration d'une des nombreuses conjectures d'Erdös concernant les nombres puissants.

Nous consacrons une grande partie de cette thèse aux aspects numériques et expérimentaux des conjectures *abc* et de Szpiro. Pour cela, nous étudions les équations de Pell, les équations de Thue et la résolution des congruences modulo une grande puissance d'un nombre premier. A ce propos, nous décrivons des méthodes efficaces pour les résoudre et nous donnons une nouvelle démonstration de la validité de l'algorithme de Cornacchia. Nous appliquons d'abord ces méthodes pour étudier les nombres de Ramanujan (problème des Taxicabs) découvrant ainsi de nouvelles familles de ces nombres. Nous appliquons ensuite ces méthodes pour déterminer des exemples de courbes elliptiques ayant un rapport de Szpiro assez élevé par rapport à sa valeur conjecturale.

Enfin, nous consacrons une part importante à la recherche d'exemples de triplets pour la conjecture *abc*. Nous avons ainsi découvert un grand nombre de ces triplets ayant un rapport d'Oesterlé-Masser assez élevé par rapport à sa valeur conjecturale. Nous avons aussi découvert les meilleurs exemples de triplets d'entiers pour le rapport de Szpiro, donnant ainsi autant d'exemples de courbes elliptiques qui se distinguent de la forme prévue par les conjectures de Szpiro.

MOTS CLÉS: Courbes Elliptiques, Conjectures de Szpiro, Conjecture *abc*, Relations *abc*, Equations Diophantiennes, Congruences, Fractions Continues, Algorithmes, Complexité, Nombres de Ramanujan, Nombres premiers, Factorisation des entiers, Nombres puissants.