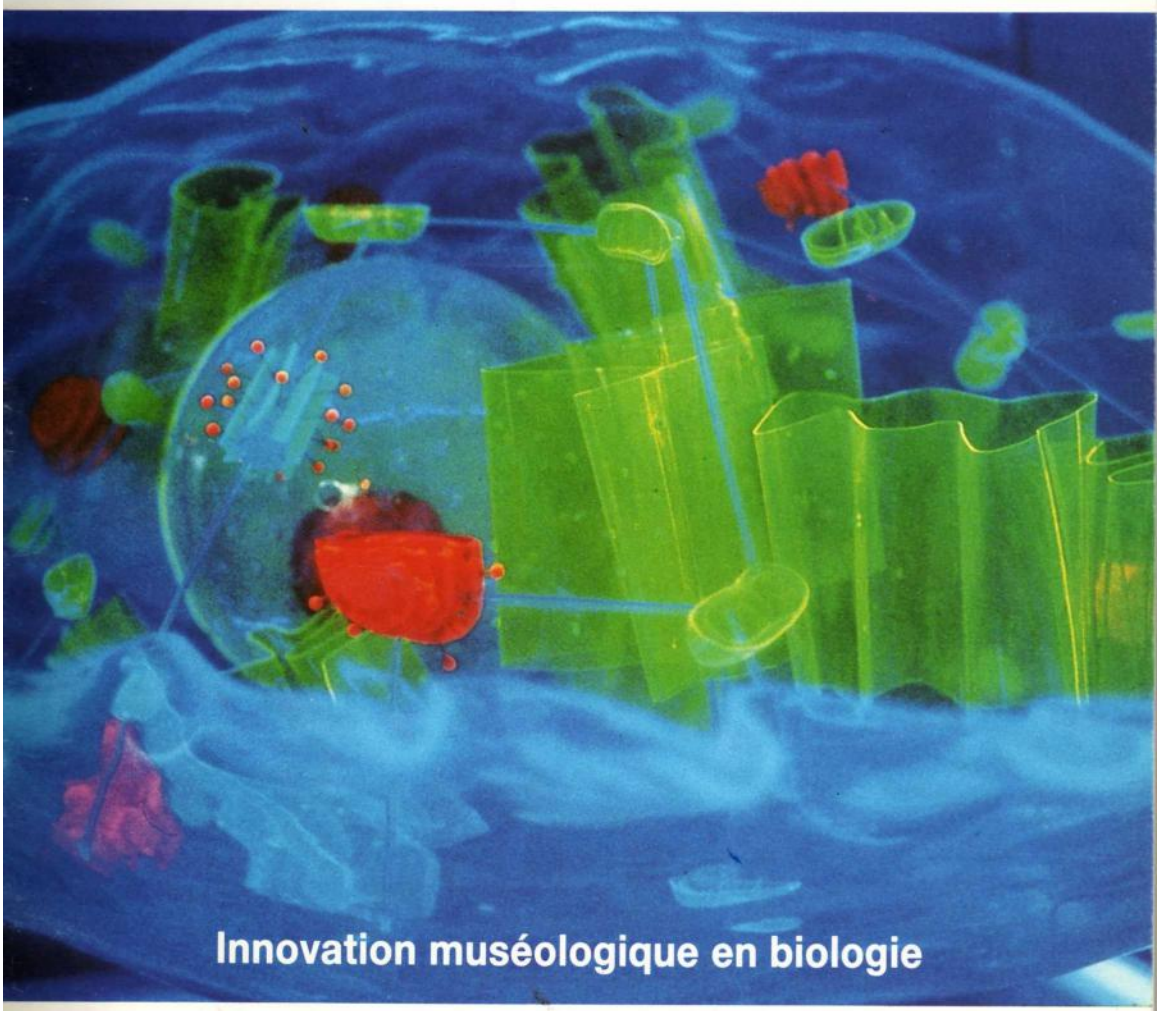
REVUE DU PALAIS DE LA

découverte

Équations diophantiennes et nombres transcendants

Traumatismes complexes de la main



Innovation muséologique en biologie

MENSUEL VOL. 15 N° 144 JANVIER 1987 15 F

équations diophantiennes et nombres transcendants

par Michel WALDSCHMIDT

Professeur à l'Université Pierre et Marie Curie (Paris VI)

Résumé. — Les pythagoriciens étudiaient les nombres incommensurables, Anaxagore la quadrature du cercle, Archimède les approximations de π, et Diophante d'Alexandrie les équations en nombres entiers. Ces différentes questions font partie de ce qu'on appelle maintenant les problèmes diophantiens, et les liens qui les unissent sont très intéressants.

Les méthodes transcendantes permettent d'établir des minorations de quantités faisant intervenir des nombres algébriques, ou même simplement rationnels, comme

$$\left| q^3\sqrt{2} - p \right| \qquad \text{ou} \qquad \left| a_1^{b_1} \dots a_n^{b_n} - 1 \right|$$

avec p, q, a_i, b_i entiers. Ces minorations servent à résoudre des équations en nombres entiers, telles que

$$x^3 - 2y^3 = k \qquad \text{ou} \qquad x^p - y^q = 1$$

(avec k entier fixé, x, y, p, q inconnues entières).

Summary. — *The Pythagoreans studied irrational numbers, Anaxagores the quadrature of the circle, Archimedes the approximations of π and Diophantus of Alexandria the diophantine equations. These questions are now included in what is referred to as « diophantine problems », and the connections between them are worth of interest.*

Transcendence methods enable us to give lower bounds for certain quantities involving algebraic or even rational numbers, such as

$$\left| q^3\sqrt{2} - p \right| \qquad \text{ou} \qquad \left| a_1^{b_1} \dots a_n^{b_n} - 1 \right|$$

with p, q, a_1, b_1 entegers.

These lower bounds provide a useful tool for solving equations in integers, such as

$$x^3 - 2y^3 = k \qquad \text{or} \qquad x^p - y^q = 1$$

where k is a fixed integer, and the unknowns x, y, p, q are also integers.

*
* *

1. Equations diophantiennes

Une « équation diophantienne » est une équation dont les coefficients et les inconnues sont des nombres entiers ou rationnels. La plus célèbre est l'équation de Fermat :

$$x^n + y^n = 1.$$

Le « théorème de Fermat » (qui n'est pas encore démontré) affirme que cette équation n'a pas de solution (x, y, n) avec x et y rationnels non nuls et n entier supérieur ou égal à 3. Nous rencontrerons plus loin l'équation de Mordell : $y^2 = x^3 + k$, l'équation de Catalan : $x^p - y^q = 1$, celle de Pillaï : $x^p - y^q = k$. L'équation : $x^3 - 2y^3 = k$ est une équation de Thue.

Quand Diophante étudiait de telles équations, il les introduisait de façon géométrique, puis cherchait à en trouver une solution. Par exemple, le problème 17 du livre VI s'énonce :

« Trouver un triangle rectangle dont la somme de l'aire et de l'hypothénuse soit un carré, et dont le périmètre soit un cube. »

Diophante choisit un des côtés de l'angle droit de longueur 2 ; si c est l'hypothénuse et b l'autre côté de l'angle droit, on doit vérifier $b + c = y^2$ et $2 + b + c = x^3$, avec x, y, b, c rationnels, donc

$$y^2 = x^3 - 2.$$

Diophante trouve la solution $x = 3$, $y = 5$. Comme le triangle est rectangle, on a aussi $b^2 + 4 = c^2$, ce qui donne $b = 12{,}42$ et $c = 12{,}58$ (fig. 1).

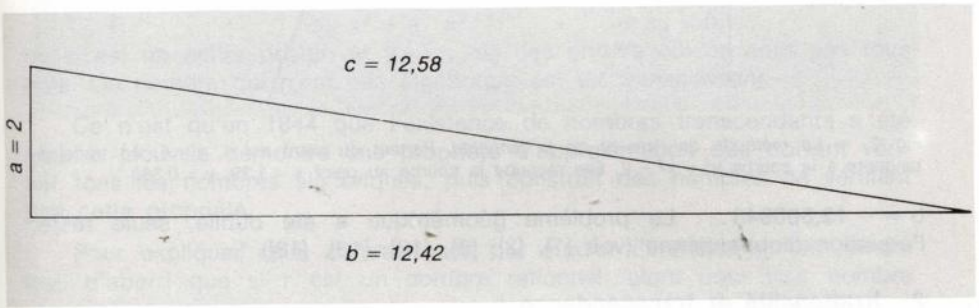


Fig. 1. — *Triangle de Diophante.* Ce triangle est rectangle : $(12{,}42)^2 + 4 = (12{,}58)^2$.
Son périmètre est un cube : $27 = 3^3$.
La somme de l'aire et de l'hypothénuse est un carré : $12{,}42 + 12{,}58 = 5^2$.

En 1621, Bachet de Méziriac a traduit et annoté l'œuvre de Diophante ; il introduisit alors la « méthode de l'arc et de la tangente » : si on dispose de deux points (x_1, y_1) et (x_2, y_2) sur la courbe $y^2 = x^3 - 2$, on trace la droite passant par ces deux points ; elle recoupe la courbe en un troisième point (x_3, y_3) à coordonnées rationnelles. Si on dispose d'un seul point au départ, on trace la tangente à la courbe en ce point (fig. 2). Il est intéressant de noter que la solution rationnelle $x = 1{,}29$, $y = 0{,}383$, obtenue par la méthode de la tangente à partir du point $x = 3$, $y = 5$, donne pour la question initiale de Diophante une valeur négative pour le côté b :

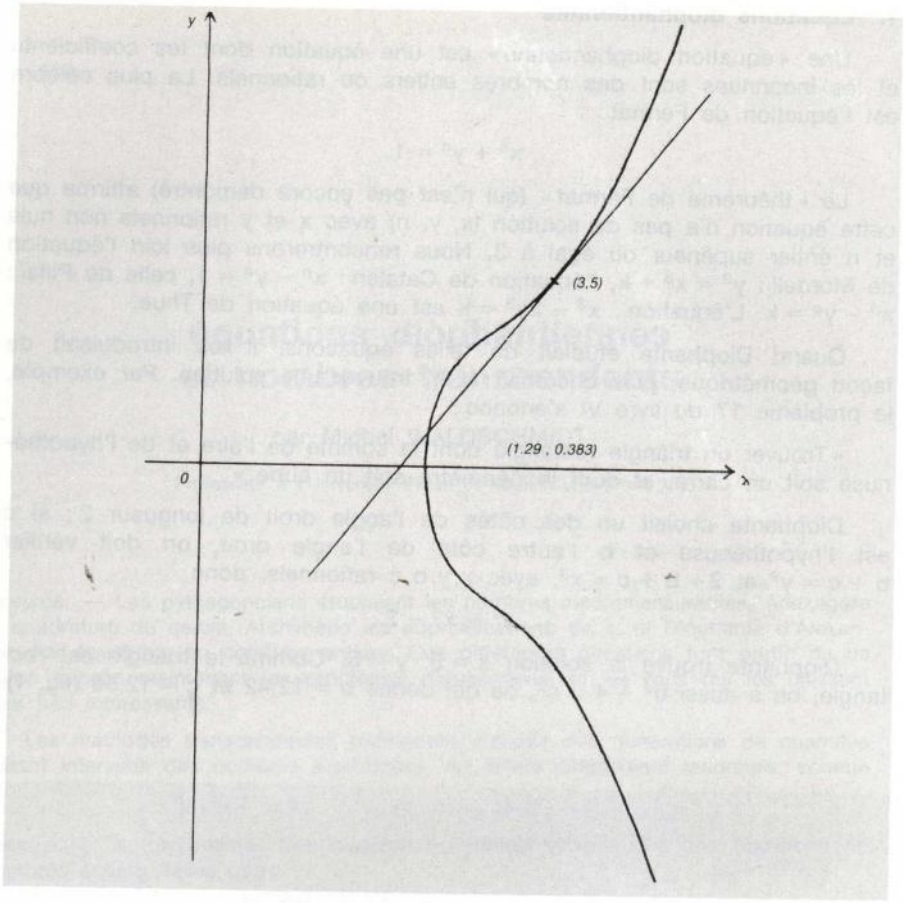


Fig. 2. — *La méthode de l'arc et de la tangente.* Partant du point $x = 3$, $y = 5$, on trace la tangente à la courbe $y^2 = x^3 - 2$. Elle recoupe la courbe au point $x = 1{,}29$, $y = 0{,}383$.

$b = -13{,}560943\ldots$ Le problème géométrique a été oublié, seule reste l'équation diophantienne (voir [1], [2], [8], [12], [13], [18]) *.

2. Irrationalité et transcendance

Pour les mathématiciens grecs, les nombres servaient à mesurer des grandeurs géométriques. Ils savaient, depuis le philosophe pythagoricien Hippasus de Metapontum ([6], [7]), que $\sqrt{2}$, diagonale du carré de côté unité, n'est pas un nombre rationnel. A la même époque, Anaxagore posait le problème de la quadrature du cercle : il s'agit de construire à la règle et au compas un carré dont l'aire soit égale à celle d'un disque donné. Plus tard, Archimède montrera que ce problème est équivalent à celui de la rectification du cercle, c'est-à-dire la construction d'un segment de longueur égale à la circonférence d'un disque donné. Archimède avait aussi étudié les approximations du nombre π en remplaçant le cercle par des polygones réguliers ([4], [5]).

* Les références entre crochets se trouvent p. 23-24.

C'est seulement au XVIII[e] siècle que des méthodes puissantes pour démontrer l'irrationalité de certains nombres vont être développées. Euler, en 1737, étudie le nombre e, base des logarithmes népériens :

$$e = \sum_{n \geq 0} \frac{1}{n!} = 1 + \frac{1}{1} + \frac{1}{1.2} + \frac{1}{1.2.3} + \frac{1}{1.2.3.4} + \ldots$$

$$= 2{,}718281828459\ldots$$

qu'il développe en fraction continue

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ldots}}}$$

que l'on écrit

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \ldots, 2n, 1, 1, 2n + 2, 1, 1, \ldots]$$

et il en déduit l'irrationalité de ce nombre.

Un peu plus tard, Lambert obtiendra par des méthodes similaires l'irrationalité d'autres constantes, par exemple celle de π, et il souligne l'intérêt de ce résultat en vue d'une solution négative du problème de la quadrature du cercle. En effet, les constructions à la règle et au compas ne peuvent produire que des nombres vérifiant certaines équations. En particulier, tous les nombres ainsi obtenus sont *algébriques*, c'est-à-dire solutions d'une équation de la forme

$$a_0 x^d + a_1 x^{d-1} + \ldots + a_d = 0, \qquad (2.1)$$

où d est un entier positif, et $a_0, \ldots, a_d$ des entiers qui ne sont pas tous nuls. Un nombre qui n'est pas algébrique est dit *transcendant*.

Ce n'est qu'en 1844 que l'existence de nombres transcendants a été établie. Liouville démontre une propriété d'approximation que doivent vérifier tous les nombres algébriques, puis construit des nombres ne vérifiant pas cette propriété.

Pour expliquer cela, commençons par étudier l'irrationalité. On remarque d'abord que si r est un nombre rationnel, alors pour tout nombre rationnel $\frac{p}{q}$ distinct de r (avec p et q entiers, $q > 0$) on a

$$\left| r - \frac{p}{q} \right| \geq \frac{c}{q} \qquad (2.2)$$

où c est un nombre positif ne dépendant que de r.

Pour démontrer (2. 2), on écrit $r = \frac{a}{b}$, avec a et b entiers, $b > 0$, et on remarque que $aq - bp$ est un entier non nul, donc en valeur absolue supérieur ou égal à 1 :

$$\left| r - \frac{p}{q} \right| = \left| \frac{a}{b} - \frac{p}{q} \right| = \left| \frac{aq - bp}{bq} \right| \geq \frac{1}{bq},$$

ce qui donne le résultat annoncé avec $c = \frac{1}{b}$.

Par conséquent, si x est un nombre pour lequel il existe une suite de rationnels p_n/q_n, $(n \geqslant 0)$, tous distincts de x, telle que $| q_n x - p_n |$ tende vers 0 avec n, alors x est irrationnel. Ainsi, pour $x = e$, on peut choisir

$(p_0/q_n) = (1, 1)$, $(p_1, q_1) = (2, 1)$, $(p_2, q_2) = (5, 2)$, $(p_3, q_3) = (16, 6)$,

et généralement

$$q_n = n! = 1 . 2 . 3 \ldots n = nq_{n-1},$$

$$p_n = n! \sum_{h=0}^{n} \frac{1}{h!} = n! + \frac{n!}{1!} + \frac{n!}{2!} + \ldots + \frac{n!}{(n-1)!} + \frac{n!}{n!} = np_{n-1} + 1 ;$$

on trouve facilement

$$0 < q_n e - p_n < \frac{2}{n+1} \quad \text{pour tout } n \geqslant 0,$$

ce qui donne l'irrationalité de e (cette démonstration a été donnée par Fourier en 1815).

L'inégalité de Liouville est une variante de (2. 2), non plus seulement pour des nombres r rationnels, mais plus généralement pour des nombres algébriques.

Théorème de Liouville : si α est une racine de l'équation (2. 1), alors pour tout nombre rationnel p/q (avec p et q entiers, $q > 0$) différent de α on a

(2. 3) $$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{c(\alpha)}{q^d},$$

où $c(\alpha)$ est un nombre positif ne dépendant que de α.

Quand $d = 1$, on retrouve l'inégalité (2. 2). Pour $d = 2$, on peut démontrer (2. 3) en utilisant les fractions continuées ([14], th. 188). Mais pour $d \geqslant 3$ un autre argument est nécessaire. Démontrons par exemple que pour tout rationnel p/q on a

(2. 4) $$\left| \sqrt[3]{2} - \frac{p}{q} \right| \geqslant \frac{1}{6q^3},$$

c'est-à-dire que l'on peut choisir dans (2. 3) $c(\alpha) = \frac{1}{6}$ quand $\alpha = \sqrt[3]{2}$.

On vérifie d'abord que (2. 4) est vraie si $p/q \geqslant 3/2$: en effet

et $$\sqrt[3]{2} = 1{,}259921 \ldots$$

$$\frac{3}{2} - \sqrt[3]{2} > 0{,}24 > \frac{1}{6} \geqslant \frac{1}{6q^3}.$$

On peut donc supposer $0 < p < \frac{3}{2} q$. Comme $\sqrt[3]{2}$ est irrationnel, l'entier $p^3 - 2q^3$ n'est pas nul, donc a une valeur absolue supérieure ou égale à 1. Mais $p^3 - 2q^3 = (p - \sqrt[3]{2}q)(p^2 + pq\sqrt[3]{2} + q^2\sqrt[3]{4})$ et notre hypothèse $p < \frac{3}{2} q$ donne

$$p^2 + pq\sqrt[3]{2} + q^2\sqrt[3]{4} < 6q^2.$$

En regroupant, on retrouve

$$1 \leqslant \left| p^3 - 2q^3 \right| \leqslant \left| p - \sqrt[3]{2}\, q \right| . 6q^2$$

d'où

$$\left| p - \sqrt[3]{2}\, q \right| \geqslant 1/6q^2 ,$$

ce qui démontre (2. 4).

Liouville utilise son théorème pour construire des nombres transcendants : le nombre

$$\sum_{n \geqslant 1} 10^{-n!} = 10^{-1} + 10^{-2} + 10^{-6} + 10^{-24} + \ldots$$

$$= 0{,}1100010 \ldots$$

ne vérifie pas d'inégalité de la forme (2. 3), quels que soient les choix de c (α) et de d, donc il est transcendant.

La transcendance du nombre e a été démontrée par Hermite en 1873, celle de π par Lindemann en 1882, ce qui résolvait définitivement la question de la quadrature du cercle ([2], [3], [4], [5], [9], [11] pour des aperçus historiques).

3. Approximations diophantiennes et équations diophantiennes

Au siècle dernier, seules les équations de degré un ou deux en deux inconnues

$$ax + by = c, \qquad ax^2 + by^2 + cxy + dx + ey + f = 0$$

(avec a, b, c, d, e, f entiers fixés, x, y inconnues entières) étaient résolues. Les équations linéaires avaient été résolues par l'astronome hindou Aryabhata dès le VI^e siècle [8], alors que l'étude des points entiers sur des coniques, commencée par Brahmagupta au VII^e siècle [8] pour l'équation

$$x^2 - dy^2 = b$$

(appelée en Occident équation de Pell-Fermat), a été achevée par Euler et Lagrange.

Pour les équations de degré supérieur, on connaissait de nombreux exemples (travaux de Fermat, Euler, Gauss notamment), mais aucune théorie générale n'avait pu être élaborée.

Sous l'influence de Hilbert, Hurwitz et Poincaré, Mordell et Weil vont introduire des outils de géométrie algébrique qui se révéleront remarquablement efficaces pour l'étude des points rationnels, avec notamment les résultats de Faltings en 1983 (voir encadré).

Mais les premiers énoncés généraux concernant les équations diophantiennes ont été obtenus au début de ce siècle grâce à des méthodes d'approximation. Le mathématicien norvégien Axel Thue obtint en 1908 une amélioration de l'inégalité (2. 3) de Liouville. Il remplace dans la partie droite de cette inégalité l'exposant d par un exposant inférieur à d, et il en déduit l'énoncé suivant : soient d un entier supérieur ou égal à 3, k un entier non nul, et $a_0, \ldots a_d$ des entiers. Alors l'équation

(3. 0) $$a_0x^d + a_1x^{d-1}y + \ldots + a_{d-1}xy^{d-1} + a_dy^d = k$$

n'a qu'un nombre fini de solutions entières x, y.

Le théorème de Faltings

Ce résultat, conjecturé par Mordell en 1923 et démontré par Faltings 60 ans plus tard, donne un critère pour qu'une équation diophantienne f (x, y) – 0 (où f est un polynôme à coefficients entiers en deux indéterminées) ait un nombre fini ou infini de solutions rationnelles (x, y). Si f possède un facteur de degré 1 (équation linéaire), 2 (conique) ou 3 (courbes elliptiques), l'équation peut avoir un nombre infini de solutions rationnelles, et Faltings dit que ce sont les seuls cas, après transformations convenables (« birationnelles ») des variables. En terme plus précis, si f est irréductible et si le « genre » de la courbe f (x, y) = 0 est au moins deux, alors il n'y a qu'un nombre fini de points rationnels sur cette courbe [18]. Le seul résultat aussi général précédemment connu était celui de Siegel (1929), dont la démonstration utilisait la méthode de Thue, et qui concernait les points entiers : il n'y a alors que les équations de degré 1 ou 2 (ou plus précisément les courbes de genre 0) à exclure.

On sait donc maintenant que pour chaque $n \geqslant 3$, il n'y a qu'un nombre fini de couples (x, y) de nombres rationnels tels que $x^n + y^n = 1$. Il semble que la méthode de Faltings permette d'espérer, dans un avenir proche, donner une borne pour le nombre de ces couples (x, y), mais il est plus difficile d'obtenir une borne pour les numérateurs et dénominateurs de ces nombres, x, y.

Voici un exemple. En utilisant des méthodes transcendantes inspirées par celles de Thue, on peut établir ([16] p. 46) :

$$(3.1) \qquad \left| \sqrt[3]{2} - \frac{p}{q} \right| \geqslant \frac{1}{10^6\, q^{2,955}},$$

ce qui améliore (2. 4) quand q est grand ($q \geqslant 10^{117}$). On ne peut pas expliquer ici la démonstration de (3. 1), mais nous allons seulement en déduire l'énoncé suivant : *toute solution entière* (x, y) *de l'équation*

$$(3.2) \qquad x^3 - 2y^3 = k$$

vérifie

$$|x| \leqslant 10^{137} . |k|^{23}.$$

Cet énoncé est vrai pour k = 0 : comme $\sqrt[3]{2}$ est irrationnel, la seule solution entière de $x^3 - 2y^3 = 0$ est x = y = 0. Prenons maintenant k entier non nul. On écrit (3. 2) sous la forme

$$(x - \sqrt[3]{2}\, y)\,(x^2 + \sqrt[3]{2}\, xy + \sqrt[3]{4}\, y^2) = k$$

mais $$\frac{1}{4} x^2 + \sqrt[3]{2}\, xy + \sqrt[3]{4}\, y^2 = \left(\frac{1}{2} x + \sqrt[3]{2}\, y\right)^2 \geqslant 0,$$

donc $$x^2 + \sqrt[3]{2}\, xy + \sqrt[3]{4}\, y^2 \geqslant \frac{3}{4} x^2$$

et $$|x - \sqrt[3]{2}\, y| \leqslant \frac{4}{3} \frac{|k|}{x^2}.$$

On remarque enfin que l'on a $|y| \leqslant |x|$ dès que $|x| \geqslant |k|$. L'inégalité (3. 1) donne alors

$$|x|^{0,045} < \frac{4}{3} . 10^6 \, |k|,$$

ce qui implique le résultat annoncé.

La borne obtenue est assez élevée, mais en calculant sur ordinateur le développement en fraction continuée de $\sqrt[3]{2}$, on peut effectivement déterminer toutes les solutions de l'équation (3. 2) quand | k | n'est pas trop grand ([10] p. 40).

Malheureusement, la méthode de Thue ne permet pas toujours d'obtenir une inégalité aussi explicite que (3. 1), et souvent ne permet d'obtenir qu'une borne pour le nombre de solutions d'une équation donnée. Cela ne permet pas en général de résoudre complètement cette équation. Nous allons voir une autre méthode transcendante qui donne des résultats effectifs dans des cadres généraux.

4. Logarithmes de nombres algébriques

Dans son introduction à l'analyse infinitésimale en 1748, Euler définit l'exponentielle et le logarithme. Choisissant une base a positive, on définit a^x pour x positif par

$$a^x = a \ldots a \text{ (x fois) si x est entier,}$$

et $$a^x = \sqrt[q]{a^p} \quad \text{si } x = p/q \text{ est rationnel,}$$

de sorte que $$(a^{p/q})^q = a^p .$$

Enfin, si x est réel positif on peut définir a^x par continuité :

$$a^x = \lim a^{p_n/q_n} \text{ pour } p_n/q_n \longrightarrow x$$

on définit aussi

$$a^0 = 1 \quad \text{et} \quad a^{-x} = 1/a^x .$$

Le logarithme de base a est la fonction inverse de a^x :

$$\text{si } y = a^x, \text{ on écrit } x = \log_a y.$$

Euler termine le chapitre consacré à ce sujet en affirmant : « Si un nombre y n'est pas puissance de la base a, son logarithme ne sera pas non plus irrationnel. En effet, si on avait

$$\log_a y = \sqrt{n},$$

on aurait alors

$$a^{\sqrt{n}} = y ,$$

ce qui est impossible si les nombres a et y sont rationnels. Donc, ces logarithmes qui ne sont pas puissance de la base a seront nommés à juste titre « transcendants ».

Le mot « transcendant » avait été utilisé avant, notamment par Leibniz.

Contrairement à ce que laisse entendre Euler, l'irrationnalité de $a^{\sqrt{n}}$ (pour a rationnel positif et n entier positif non carré parfait) n'est pas une chose évidente, et D. Hilbert reprit cette question dans un exposé donné au congrès international de Paris en 1900. Il présentait 23 problèmes de différentes branches des mathématiques, dont on pouvait attendre qu'ils fassent avancer cette science.

Le septième problème pose la question de l'irrationalité de $2^{\sqrt{2}}$, et plus généralement de nombres de la forme α^β, quand α et β sont des nombres algébriques, avec $\alpha \neq 0$, $\alpha \neq$ et β irrationnel. Le changement de variable

$$a_1 = \alpha, \quad a_2 = \alpha^\beta, \quad b = \beta$$

permet d'écrire ce problème sous la forme équivalente suivante :

si a_1 et a_2 sont des nombres algébriques non nuls, alors le nombre

$$\log a_1 / \log a_2$$

est soit rationnel, soit transcendant.

Quand a_1 et a_2 sont positifs, dire que $\log a_1 / \log a_2$ est rationnel revient à dire que $a_1^p = a_2^q$ avec p et q entiers non tous deux nuls.

Ce problème a été résolu par Gel'fond et Schneider en 1934. Dans une série de travaux jusqu'en 1950, Gel'fond a utilisé sa méthode pour donner des minorations de

$$\left| \frac{\log a_1}{\log a_2} - \frac{p}{q} \right|$$

Quintes et octaves

Pour sa théorie de la musique, Pythagore avait été amené à étudier la proximité d'une puissance de 2 à une autre puissance de 3.

On obtient une octave (rapport de fréquence 2) en faisant vibrer une corde de longueur moitié de la corde initiale, et une quinte (rapport de fréquence 3, ou 3/2 si on se ramène à l'octave) avec une corde de longueur un tiers. Mais des quintes successives ne permettent pas de retrouver la note initiale, car pour tout m, n entiers positifs on a

$$(\frac{3}{2})^m \neq 2^n.$$

Pour obtenir une approximation, on peut chercher une puissance de 2 qui soit proche d'une puissance de 3. C'est pourquoi au Moyen âge, Philippe de Vitry s'était intéressé à l'équation

$$3^p = 2^q \pm 1,$$

dont les seules solutions sont

$$3 = 2 + 1 \quad \text{et} \quad 9 = 8 + 1.$$

Une autre voie est d'étudier le développement en fraction continuée de $\log 3 / \log 2$:

$$\frac{\log 3}{\log 2} = [1, 1, 1, 2, 2, 3, 1, 5, \ldots]$$

qui fournit les approximations : 1 ; 2 ; $\frac{3}{2} = 1{,}5$;

$$\frac{8}{5} = 1{,}6 \; ; \; \frac{19}{12} = 1{,}5833\ldots \text{ de } \frac{\log 3}{\log 2} = 1{,}58496\ldots$$

Cette dernière approximation $\frac{19}{12}$ conduit à une gamme tempérée de 12 notes, avec comme demi-ton un rapport $2^{1/12}$, et la quinte a une fréquence relative de $2^{7/12} = 1{,}4983\ldots$ au lieu de $\frac{3}{2} = 1{,}5$.

Les inégalités obtenues par les méthodes transcendantes donnent une limite à la qualité des gammes qu'on peut ainsi obtenir :

$$\left| \frac{\log 3}{\log 2} - \frac{p}{q} \right| > q^{-15} \text{ . pour } q \geqslant 2 \text{ .}$$

On notera en passant que le nombre transcendant $\frac{\log 3}{\log 2}$ n'est pas un nombre de Liouville, c'est-à-dire que le fait qu'il soit transcendant ne peut pas être déduit de (2. 3).

quand $\log a_1 / \log a_2$ est irrationnel. Cela revient à minorer

$$| q \log a_1 - p \log a_2 | \text{ .}$$

Il a donné des applications intéressantes de ces minorations, et a mis en

évidence l'intérêt qu'aurait une généralisation à une minoration d'une expression de la forme

$$| b_1 \log a_1 + \ldots + b_n \log a_n | .$$

Le cas particulier le plus intéressant est aussi le plus simple : $a_1, \ldots, a_n$ sont des entiers positifs. Cela revient à minorer

$$| a_1^{b_1} \ldots a_n^{b_n} - 1 | ,$$

et ce problème a été résolu par Baker en 1966.

La minoration évidente est

$$(4.1) \qquad \left| a_1^{b_1} \ldots a_n^{b_n} - 1 \right| \geqslant \frac{1}{A^{nB}},$$

avec $A = \max a_i$, et $B = \max b_i$, sous la seule hypothèse $a_1^{b_1} \ldots a_n^{b_n} \neq 1$. Il suffit de remarquer que le membre de gauche de (4. 1) est un nombre rationnel de dénominateur majoré par A^{nB}. La démonstration est donc de même nature que celle du théorème de Liouville (2. 3).

Les derniers travaux sur la méthode de Baker permettent d'établir pour $B \geqslant 2$:

$$(4.2) \qquad | a_1^{b_1} \ldots a_n^{b_n} - 1 | \geqslant B^{-C_1 (\log A_1) \ldots (\log A_n)}$$

avec $A_i = \max (a_i, 2)$, et C_1 est une constante positive ne dépendant que de n (et qu'on peut calculer explicitement).

Cette inégalité (4. 2) est meilleure que (4. 1) quand B est grand (ce qui est le cas dans les applications). Mais elle est encore loin de ce que l'on peut espérer.

Prenons comme hypothèse de travail l'inégalité ([17]) :

$$(4.3) \qquad \left| a_1^{b_1} \ldots a_n^{b_n} - 1 \right| \geqslant \frac{1}{(AB)^{C_2}}$$

avec une constante $C_2 > 0$ ne dépendant que de n, et montrons l'intérêt qu'aurait une telle estimation. Considérons le premier cas intéressant : $n = 2$, b_1 et b_2 de signes contraires. Nous allons en déduire la :

Conjecture de Pillaï : soit k *un entier positif. L'équation*

$$(4.4) \qquad x^p - y^q = k$$

n'a qu'un nombre fini de solutions en entiers (x, y, p, q) *tous supérieurs ou égaux à* 2.

Si p est fixe, $\geqslant 2$, on sait que l'équation $y^q = x^p - k$ n'a qu'un nombre fini de solutions (x, y, q) avec $q \geqslant 3$. Cela a été démontré (sous une forme plus générale : on peut remplacer $x^p - k$ par tout polynôme ayant au moins deux racines distinctes et simples ; [15] p. 64) par Schinzel et Tijdeman en utilisant des inégalités provenant de la méthode de Baker (4. 2). Le cas $p = q = 2$, étant banal, on pourra donc supposer p et q tous les deux grands. On va supposer précisément :

$$(4.5) \qquad p^{3C_2} \leqslant 2^p \qquad \text{et} \qquad q^{3C_2} \leqslant 2^q.$$

En particulier $p \geqslant 3C_2$ et $q \geqslant 3C_2$. Ecrivons alors

$$x^{-p} y^q - 1 = \frac{-k}{x^p},$$

et utilisons (4. 3) avec

$$a_1 = x, \; a_2 = y, \; b_1 = -p, \; b_2 = q .$$

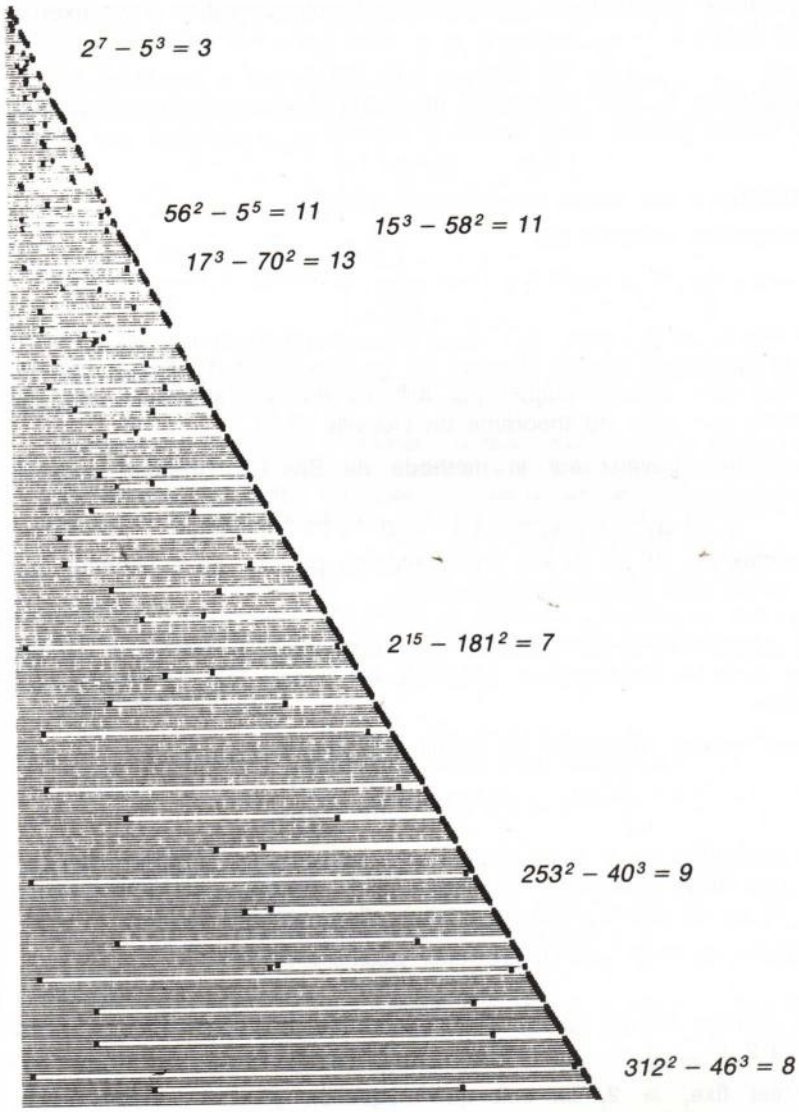


Fig. 3. — *La conjecture de Pillaï.* Les puissances parfaites sont les nombres de la forme x^p, avec x et p entiers, $x \geqslant 1$, $p \geqslant 2$. La conjecture de Pillai signifie que la distance de deux puissances parfaites consécutives tend vers l'infini. Voici le début de cette suite :

1 4 8 9 16 25 27 32 36 49 64 81 100 121 125 128 144 169
196 216 225 243 256 289 324 343 361 400 441 484 512 529 576
625 676 729 784 841 900 961 1 000.

Le diagramme suivant (fourni par Eric Reyssat grâce à l'ordinateur de l'UA 763) montre les différences entre les puissances parfaites consécutives. Le début de cette suite est :

3 4 1 7 9 2 5 4 13 15 17 19 21 4 3 16 25 27 20 9 18
13 33 35 19 18 39 41 43 28 17 47 49 51 53 55 57 59 61 39

Les différences les plus grandes n'apparaissent évidemment qu'entre deux carrés qui ne sont séparés par aucune autre puissance parfaite, ce qui est le cas le plus fréquent. Dans l'intervalle considéré, on constate que les différences les plus petites n'apparaissent que quand un cube est voisin d'un carré. La conjecture de Hall dit que de telles différences ne devraient jamais être « trop petites », et on conjecture aussi que pour les exposants autres que 2 et 3 les différences sont encore plus grandes.

On trouve

$$\frac{k}{x^p} \geqslant \left| x^{-p}y^q - 1 \right| \geqslant \frac{1}{(AB)^{C_2}}$$

avec

$$A = \max(x, y) \text{ et } B = \max(p, q),$$

donc

(4. 6) $$x^p < k\,(AB)^{C_2}.$$

Comme $p \geqslant 3C_2$, on a

$$x^{C_2} \leqslant x^{p/3}.$$

Puisque $q \geqslant 3C_2$ et $x^p > y^q$, on a aussi

$$y^{C_2} < x^{\frac{p}{q}C_2} \leqslant x^{p/3}.$$

Ainsi

$$A^{C_2} \leqslant x^{p/3}.$$

D'autre part, comme $x \geqslant 2$, on déduit de (4. 5)

$$p^{C_2} \leqslant 2^{p/3} \leqslant x^{p/3},$$

et de même

$$q^{C_2} \leqslant 2^{q/3} \leqslant y^{q/3} < x^{p/3},$$

ce qui donne

$$B^{C_2} \leqslant x^{p/3}.$$

Alors (4. 6) permet de conclure que toute solution de (4. 4) satisfait

$$y^q < x^p \leqslant k^3.$$

Le seul cas où la conjecture de Pillaï soit résolue est $k = 1$. Tijdeman a démontré il y a une dizaine d'années qu'il existe une constante absolue $C_3 > 0$ telle que toute solution (x, y, p, q) en entiers $\geqslant 2$ de l'équation

(4. 7) $$x^p - y^q = 1$$

vérifie

$$x^p \leqslant C_3.$$

Mais la valeur numérique de C_3 est énorme et on ne sait pas encore résoudre la *conjecture de Catalan*, selon laquelle la seule solution de (4. 7) est

$$x = 3,\ p = 2,\ y = 2,\ q = 3.$$

Les inégalités de la méthode de Baker telles que (4. 2) permettent de résoudre de nombreuses équations diophantiennes. Par exemple Baker [16] a montré que toute solution (x, y) en entiers de l'équation $y^2 = x^3 + k$, pour $k \neq 0$, vérifie

(4. 8) $$\max(|x|, |y|) \leqslant \exp(10^{10}\,|k|^{10000}).$$

D'un point de vue théorique, il est intéressant de connaître une telle borne explicite. D'un point de vue pratique, il faut dire que la méthode permet de résoudre effectivement certaines équations, pourvu que les coefficients ne soient pas trop grands. Bien entendu, on n'applique pas directement la borne (4. 8), mais on effectue dans chaque cas un travail théorique qui n'est pas négligeable. Ensuite, pour chaque valeur de $|k|$ inférieure à 1000, il faut moins de cinq minutes à un ordinateur pour compléter la liste des solutions de l'équation de Mordell $y^2 = x^3 + k$. De même pour les

Quelques problèmes ouverts

• Le plus célèbre (Fermat) : pour chaque entier $n \geqslant 3$, l'équation $x^n + y^n = z^n$ ne possède pas de solution en entiers x, y, z strictement positifs.

• La conjecture de Catalan : 8 et 9 sont les seuls entiers consécutifs qui soient des puissances parfaites.

• La conjecture de Pillaï : pour chaque entier $k \geqslant 1$, il n'y a qu'un nombre fini de puissances parfaites x^p telles que $x^p + k$ soit aussi une puissance parfaite.

• On ne connaît pas d'algorithme permettant de dire si une équation

$$f(x, y) = 0$$

a une solution entière (x, y), quand f est un polynôme à coefficients entiers :

$$f(x,y) = a_{00} + a_{01}\, x + a_{10}\, y + a_{02}\, x^2 + a_{11}\, xy + a_{20}\, y^2 + \ldots + a_{0d}\, x^d + a_{1,d-1}\, x^{d-1}\, y + \ldots + a_{d-1,1}\, xy^{d-1} + a_{d,0}\, y^d .$$

S'il y a une solution entière, il n'y a pas d'algorithme connu permettant de les trouver toutes. Les mêmes problèmes se posent pour les solutions rationnelles. Si on augmente le nombre de variables, on sait qu'il n'y a pas d'algorithme (10e problème de Hilbert).

(*) • On sait majorer le nombre N de solutions d'une équation de Thue

$$a_0 x^d + a_1 x^{d-1} y + \ldots + a_d y^d = 1$$

en fonction de d seulement (travaux récents d'Evertse, Bombieri et Schmidt). Siegel a suggéré en 1929 que N pourrait être majoré en fonction du nombre des coefficients non nuls a_i. Par exemple, existe-t-il une constante absolue $C > 0$ telle que pour tout d, i, a, b entiers avec $d > i \geqslant 2$, l'équation :

$$x^d + ax^{d-i}y^i + by^d = 1$$

ait au plus C solutions ?

• Conjecture de Hall ([1], [17]). Existe-t-il une constante $C > 0$ telle que pour tout x, y entiers positifs vérifiant $x^2 \neq y^3$, on ait

$$x^2 - y^3 > C \max (x^2, y^3)^{1/6} ?$$

On sait seulement démontrer (par la méthode transcendante de Baker) des minorations faisant intervenir une puissance positive de max (log x, log y), au lieu d'une puissance positive de max (x^2, y^3).

• Conjecture abc (Œsterlé - Masser). Existe-t-il une constante absolue $K > 0$ ayant la propriété suivante : soient a et b deux entiers positifs premiers entre eux, soit $c = a + b$, et soit P le produit des nombres premiers qui divisent abc ; alors

$$c < P^K$$

Voici deux exemples numériques qui montrent que la constante K, si elle existe, doit être au moins égale à 1,62 :

(De Weger) : $a = 3^2 5^6 7^3$, $b = 11^2$, $c = 2^{21} 23$.

(Reyssat) : $a = 3^{10} 109$, $b = 2$, $c = 23^5$.

Cette conjecture abc permettrait de résoudre beaucoup de problèmes, par exemple le problème de Fermat (pour $n > 3K$) et la conjecture de Pillaï.

(*) Ce problème a été résolu au printemps 1986, par J. Mueller et W.M. Schmidt.

équations de Thue (3. 0), on dispose maintenant d'algorithmes permettant de trouver toutes les solutions entières quand les paramètres d, $a_0, \ldots, a_d$, k ne sont pas trop grands.

Conclusion

Les principaux algorithmes généraux pour résoudre en nombres entiers des équations diophantiennes en deux indéterminées de degré au moins 3 proviennent de méthodes de la théorie des nombres transcendants.

Le théorème de Faltings, qui n'utilise pas de résultat d'approximation diophantienne, mais repose sur des techniques de géométrie algébrique, fournit un critère pour qu'une telle équation diophantienne ait un nombre fini de solutions rationnelles. Il reste encore à les trouver toutes effectivement.

Il est difficile de prédire quelle méthode s'avérera la plus efficace. Les problèmes ouverts ne manquent pas, les progrès récents sont importants, et on peut raisonnablement espérer que de nouveaux résultats seront obtenus dans un avenir proche.

M. W.

Ce sujet a fait l'objet d'une conférence prononcée au Palais de la Découverte, le 22 février 1986.

Agrégé de mathématiques en 1969, docteur ès mathématiques en 1972, Michel Waldschmidt a été successivement assistant à l'Université de Bordeaux I (1968-1971), attaché de recherche au CNRS (1971-1972), chargé d'enseignement à Orsay (1972-1973), puis maître de conférence à Paris VI (1973-1977). Depuis 1977, il est professeur à l'université Pierre et Marie Curie (Paris VI).

Auteur de nombreuses publications et de plusieurs ouvrages sur les nombres transcendants, il a créé une équipe de recherche sur les problèmes diophantiens à l'Institut Henri Poincaré qu'il dirige avec Daniel Bertrand.

Membre de plusieurs comités de rédaction, conseils scientifiques et sociétés savantes, il a été président de la première section (sciences mathématiques) de l'Association française pour l'avancement des sciences en 1983 et 1984.

références

[1] Serge LANG fait des maths en public. — 3 débats au Palais de la Découverte. Ed. Belin, 1984.

[2] M. WALDSCHMIDT et J. VELU. — Les victoires de la transcendance. *La Recherche* n° 84, déc. 1977, vol. 8, p. 1059-1065.

[3] F. GRAMAIN. — Les nombres transcendants. *Pour la Science*, n° 80, juin 1984, p. 70-79.

[4] Numéro spécial π du Petit Archimède, n° 64-65, 1980.

[5] P. DUBREIL. — L'histoire des nombres mystérieux π, e, C, i. In : Les grands courants de la pensée mathématique. Ed. Le lionnais, 1962.

[6] Ph. JONES. — Irrationals or incommensurables. The Math. Teacher 48 (1956), 49-50.

[7] Kurt von FRITZ. — The discovery of incommensurability by Hippasus of Metapontum. Annals of Math. 46 (1945), 242-264.

[8] B.L. van der WAERDEN. — Geometry and algebra in ancient civilizations. Springer-Verlag, 1984.

[9] R. FRITSCH. — The transcendance of π has been known for about a century, but who was the man who discovered it? Results in Math., 7 (1984), 165-183.

[10] D. BERTRAND et al. — Les nombres transcendants, ERA 979. Mémoire Soc. Math. France, Nouvelle série, n° 13, 1984.

[11] M. WALDSCHMIDT. — Les débuts de la théorie des nombres transcendants (à l'occasion du centenaire de la transcendance de π). Cahiers du sém. d'Histoire des Maths, 4 (1984), 93-115.

[12] L.J. MORDELL. — Diophantine equations. Academic Press, 1969.

[13] L.E. DICSON. — History of the theory of numbers. Chelsea, 1952.

[14] G.H. HARDY et E.M. WRIGHT. — The theory of numbers. Oxford, 1962.

[15] Transcendence theory, advances and applications. — Ed. A. Baker and D.W. Masser, Academic Press, 1977. Voir notamment le chap. 3 (p. 59-77) par T.N. Shorey, A.J. van der Poorten, R. Tijdeman et A. Schinzel : Applications of the Gel'fond-Baker method to diophantine equations.

[16] A. BAKER. — Transcendental number theory. Cambridge Univ. Press, 2e éd., 1979. Voir notamment le chap. 4 (p. 36-46) : Diophantine equations.

[17] S. LANG. — Elliptic curves, diophantine analysis. Springer Verlag, Grund. der Math. Wiss 231, 1978.

[18] B. MAZUR. — Arithmetic on curves. Bull. Amer. Math. Soc., 14 (1986), 207-259.