http ://www.cimpa-icpam.org/Francais/Cooperations/Ragaad.html

"Algèbre commutative -Codes correcteurs et Cryptographie"
RAGAAD Bamako, 23 novembre 2005

MÉTHODES DIOPHANTIENNES ET ALGORITHMES EFFECTIFS

par *Michel Waldschmidt*
Université P. et M. Curie (Paris VI)
http ://www.math.jussieu.fr/∼miw

Équations Diophantiennes

Exemple : $y^2 - x^3 = 1$

Diophante : $x = 2$, $y = 3$

Fermat : chercher toutes les solutions

Euler : la seule solution (x, y) de l'équation $y^2 - x^3 = \pm 1$ est $(3, 2)$.

Avant 1900 : Hilbert et Hurwitz, Poincaré.

Début du XXè siècle : Thue. Lien avec l'approximation diophantienne.

XXè siècle : Gel'fond. Lien avec la transcendance.

Soit κ dans l'intervalle $0 < \kappa \leq 3$.
Les deux conditions suivantes sont équivalentes :

(i) Il existe $c_1 > 0$ *tel que*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{c_1}{q^\kappa}$$

pour tout $p/q \in \mathbf{Q}$.

(ii) Il existe $c_2 > 0$ *tel que*

$$|x^3 - 2y^3| \geq c_2\, x^{3-\kappa}$$

pour tout $(x, y) \in \mathbf{Z}^2$ *avec* $x > 0$.

M. Bennett : vrai avec $\kappa = 2,5$:

Pour tout $p/q \in \mathbf{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\, q^{2,5}}.$$

Pour tout $(x, y) \in \mathbf{Z}^2$ *avec* $x > 0$,

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

Résultats antérieurs :

Baker, Chudnovskii, Easton, Rickert, Voutier,...

Cas général : soit α un nombre algébrique réel de degré $d \geq 3$ et de polynôme minimal $f \in \mathbf{Z}[X]$, et soit $F(X, Y) = Y^d f(X/Y) \in \mathbf{Z}[X, Y]$ le polynôme homogène associé. Soit $0 < \kappa \leq d$. Les deux conditions suivantes sont équivalentes :
(i) Il existe $c_1 > 0$ *tel que, pour tout* $p/q \in \mathbf{Q}$,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c_1}{q^\kappa}.$$

(ii) Il existe $c_2 > 0$ *tel que, pour tout* $(x, y) \in \mathbf{Z}^2$ *avec* $x > 0$,

$$|F(x, y)| \geq c_2\, x^{d-\kappa}.$$

Questions d'effectivité

J. Liouville, 1844 : $c(\alpha) > 0$ explicite pour lequel

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d}.$$

A. Thue, 1910's : existence de $\kappa < d$ et de $c(\alpha) > 0$ avec

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^\kappa}.$$

Corollaire : nombre fini de solutions $(x, y) \in \mathbf{Z}^2$ de l'équation de Thue $F(x, y) = k$.
Majoration du nombre de solutions.

Finitude du nombre de solutions

C.L. Siegel (1929) :
nombre fini de points entiers sur une courbe de genre ≥ 1 sur un corps de nombres.

Conjecture de Mordell, résolue par G. Faltings (1983) :
nombre fini de points rationnels sur une courbe de genre ≥ 2 sur un corps de nombres.

Majoration explicite du nombre de solutions : G. Rémond (2000).

Problème ouvert : points entiers sur une courbe de genre 2.

Transcendance de α^β

1934. Solution par A.O. Gel'fond et Th. Schneider du septième problème de Hilbert.

A.O. Gel'fond : minorations de $|\alpha_1^\beta - \alpha_2|$.

Cas $\beta \in \mathbf{Q}$: minorations de

$|\alpha_1^{-b_1/b_2} - \alpha_2|$

$|\alpha_1^{b_1} - \alpha_2^{-b_2}|$

$|\alpha_1^{b_1}\alpha_2^{b_2} - 1|$.

Liouville :

$$|\alpha_1^{b_1}\alpha_2^{b_2} - 1| \geq \exp\{-c(\alpha_1, \alpha_2)B\}$$

avec $B = \max\{|b_1|, |b_2|\}$.

Gel'fond :

$$|\alpha_1^{b_1}\alpha_2^{b_2} - 1| \geq \exp\{-c(\alpha_1, \alpha_2)(\log B)^2\}.$$

Liouville :

Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls.

Il existe $c = c(\alpha_1, \ldots, \alpha_n) > 0$ *tel que, si* $b_1, \ldots, b_n$ *sont des entiers rationnels vérifiant* $\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1$ *et si* $B = \max\{|b_1|, \ldots, |b_n|\}$, *alors*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq e^{-cB}.$$

A.O. Gel'fond :

Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls et soit $\epsilon > 0$.

Il existe $B_0 = B_0(\alpha_1, \ldots, \alpha_n, \epsilon) > 0$ *tel que, si* $b_1, \ldots, b_n$ *sont des entiers rationnels vérifiant* $\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1$ *et si* $B = \max\{|b_1|, \ldots, |b_n|, B_0\}$, *alors*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq e^{-\epsilon B}.$$

Démonstration : utilise le théorème d'approximation de Thue-Siegel (+Roth-Schmidt) : non effectif.
`Remarque de M. Mignotte.`

A. Baker, N.I. Fel'dman :

Soient $\alpha_1, \ldots, \alpha_n$ des nombres algébriques non nuls.

Il existe $c = c(\alpha_1, \ldots, \alpha_n) > 0$ *tel que, si* $b_1, \ldots, b_n$ *sont des entiers rationnels vérifiant* $\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1$ *et si* $B = \max\{|b_1|, \ldots, |b_n|, 2\}$, *alors*

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq B^{-c}.$$

La constante c est effective (et même explicite dans les travaux récents).

Application de la méthode de Gel'fond-Baker à l'équation de Siegel

Théorème. *Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers, $\mathbf{Z}_K^\times$ son groupe des unités, a et b deux éléments non nuls de K. Alors l'équation*

$$au + bv = 1$$

n'a qu'un nombre fini de solutions (u, v) dans $(\mathbf{Z}_K^\times)^2$, et ces solutions peuvent être effectivement déterminées.

Corollaire. *Soient K un corps de nombres, $\alpha_1, \ldots, \alpha_m$ des éléments de K, trois au moins d'entre eux étant distincts et soit $k \in K^\times$. Alors il n'existe qu'un nombre fini de solutions (x, y) dans $\mathbf{Z}_K^2$ de l'équation*

$$(x - \alpha_1 y) \cdots (x - \alpha_m y) = k,$$

et ces solutions peuvent être effectivement déterminée

Autres équations diophantiennes résolues par cette méthode : points entiers sur une courbe de genre 1 (Baker-Coates), équations elliptiques, hyperelliptiques, superelliptiques, ...

Équation de Mordell :
(M) $y^2 = x^3 + k$
Équation elliptique
(E) $y^2 = f(x)$, $\deg f = 3$
Équation hyperelliptique :
(HE) $y^2 = f(x)$, $\deg f \geq 3$
Équation superelliptique :
(SE) $y^m = f(x)$, $m \geq 3$, $\deg f \geq 2$
Équation de Thue :
(T) $F(x, y) = k$, F homogène
Équation de Siegel :
(S) $au + bv = 1$

Conjecture de Pillai (1945) : pour tout $k \in \mathbf{Z} \setminus \{0\}$, l'équation $x^p - y^q = k$ n'a qu'un nombre fini de solutions (x, y, p, q) en entiers $x \geq 1$, $y \geq 1$, $p \geq 2$, $q \geq 2$.

Énoncé équivalent à la conjecture de Pillai : dans la suite des puissances parfaites a^b, $b \geq 2$,

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,\ \ldots$$

la différence entre deux termes consécutifs tend vers l'infini.

Conjecture de Catalan (1844) résolue par P. Mihăilescu en 2002 : l'équation $x^p - y^q = 1$ a pour seule solution $3^2 - 2^3 = 1$.

Conjecture de Hall (1971) :

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

Raffinement des conjectures de Hall et Pillai (avec S. Lang, 1978) :

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

avec

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

Lien avec l'informatique théorique : questions d'arrondis

Méthode de Gel'fond-Baker : minorations de

$$|e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n} - 1|.$$

Cas particulier :

$$|e^\beta - \alpha|$$

avec α et β algébriques.
Cas α et β rationnels, ou même entiers

$$|e^b - a|$$

Problème de Mahler : pour a et b entiers positifs,

$$|e^b - a| > a^{-c} ?$$

Conjecture plus forte :

$$|e^b - a| > b^{-c} ?$$

K. Mahler (1953, 1967), M. Mignotte (1974), Yu.V. Nesterenko+W (1996), F. Wielonsky (1997), S. Khemira (2005) :

$$|e^b - a| \geq \exp\{-1,3 \cdot 10^5 (\log A)(\log B)\}$$

où $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$.

Muller, J-M. ; Tisserand, A. –
Towards exact rounding of the elementary functions.
Alefeld, Goetz (ed.) et al.,
Scientific computing and validated numerics.
Proceedings of the international symposium on scientific computing, computer arithmetic and validated numerics SCAN-95, Wuppertal, Germany, September 26-29, 1995.
Berlin : Akademie Verlag. Math. Res. 90, 59-71 (1996).

Arithmétique des Ordinateurs,
Laboratoire de l'Informatique du Parallélisme

Computer Arithmetic — Arénaire project

http ://www.ens-lyon.fr/LIP/Arenaire/

Autres aspects de l'effectivité en analyse Diophantienne

- *Algèbre linéaire* : lemme de Siegel
- *Analyse* : lemme de Schwarz, approximants de Padé
- *Arithmétique* : théorème de Dirichlet
- *Algèbre commutative* : tests d'appartenance, théorème des zéros de Hilbert
- *Topologie* : densité
- *Courbes elliptiques* : théorème de Mordell-Weil