Astérisque

MARC HINDRY

Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)

Astérisque, tome 209 (1992), p. 39-56

<http://www.numdam.org/item?id=AST_1992__209__39_0>

SUR LES CONJECTURES DE MORDELL ET LANG (d'après VOJTA, FALTINGS et BOMBIERI).

Marc HINDRY

1 Introduction

Dans tout le texte, k désigne un corps de nombres, O_k son anneau d'entiers, C une courbe algébrique projective lisse définie sur k et g le genre de C. L'ensemble des points de C rationnels sur k est noté C(k).

On sait que:

si g=0 alors C(k) est ou bien vide ou bien en bijection avec $\mathbf{P}^1(k)$;
si g=1 alors ou bien C(k) est vide ou bien est un groupe de type fini (théorème de Mordell-Weil); la loi de groupe est par ailleurs algébrique;
si g≥2 alors C(k) est fini (Conjecture de Mordell=théorème de Faltings [F1]).
Si U est un ouvert affine de C on peut s'intéresser aux points entiers que je noterai (un peu abusivement) $U(O_k)$; on dispose alors du théorème de Siegel [Si]: $U(O_k)$ est fini sauf (peut-être) si g=0 et C–U possède au plus deux éléments. La preuve de Siegel utilise essentiellement deux ingrédients que j'explicite plus loin: a) la théorie des approximations diophantiennes (Thue-Siegel-Dyson-Gelfond-Roth-Schmidt) et b) le théorème de Mordell-Weil appliqué à la jacobienne de C.
Ces ingrédients n'apparaissent pas dans la preuve de la conjecture de Mordell par Faltings [F1] (Voir aussi les séminaires [Sz1] et [Co-Si]) même si les jacobiennes et les variétés abéliennes y jouent un rôle prépondérant. Vojta a donné une nouvelle preuve de la conjecture de Mordell dans la lignée de Siegel [V1]. Faltings , en développant les idées de Vojta a ensuite prouvé la généralisation suivante, conjecturée par Lang:

THÉORÈME 1(Faltings [F2];voir aussi [Sz2]): *Soit* X *une sous-variété d'une variété abélienne* A *définies sur* k; *on suppose que* X *ne contient aucun translaté de sous-variété abélienne non nulle, alors* X(k) *est fini.*

La preuve de Vojta [V1] utilise des idées et des techniques sophistiquées de géométrie arithmétique "à la Arakelov", notamment [G-S3]; Bombieri [B] a

simplifié cette preuve et donné une version très jolie et "presque élémentaire" du travail de Vojta; c'est un article que tout mathématicien souhaitera lire.
Les liens entre la géométrie et l'approximation diophantienne "à la Siegel" ont été développés dans plusieurs directions: Vojta a annoncé dans [V4] une inégalité plus fine que celle que nous donnons et valable sur toutes les courbes; cette inégalité contient la conjecture de Mordell et le théorème de Roth. Dans [F2] Faltings prouve une généralisation du théorème de Siegel également conjecturée par Serge Lang: un ouvert affine d'une variété abélienne ne contient qu'un nombre fini de points entiers définis sur un corps de nombres donné.
J'explicite dans cette introduction les deux ingrédients fondamentaux mentionnés ci-devant; le paragraphe suivant introduit l'outil de base de la géométrie diophantienne: les hauteurs; je donne dans les paragraphes 3 et 4 une esquisse des preuves respectivement de la conjecture de Mordell selon Vojta et du théorème 1 selon Faltings, il ne saurait donc être question d'originalité ici mais j'espère que cette présentation facilitera à certains la lecture des articles originaux décrivant ces beaux résultats. Le paragraphe 5 complète sur certains points le paragraphe 4 et décrit la conjecture générale de Serge Lang [La1] (maintenant un théorème); le dernier paragraphe raconte une application de ces résultats à l'étude des points algébriques de degré donné sur une courbe.

a)Approximations diophantiennes.
L'idée de Siegel est qu' une suite infinie de points entiers sur une courbe affine doit tendre vers l'un de ses points à l'infini (se rapprocher d'une asymptote) et donc en fournir de très bonnes approximations. Remarquons que cette remarque si simple est en défaut (au moins littéralement) si l'on travaille avec des points rationnels; on a donc longtemps cru qu'elle était inutilisable quand les points ne sont pas entiers, Vojta a montré qu'il n'en était rien.
Je donne un schéma de preuve d'inégalités de ce type (une bonne référence générale est [Sch1]):

THÉORÈME DE ROTH: *Soit* α *un nombre algébrique irrationnel et* $\kappa>2$, *alors il existe un nombre fini de solutions rationnelles à l'inégalité:*

(*) $\qquad |\alpha - \frac{p}{q}| < q^{-\kappa}.$

Premier pas: on fixe m assez grand, et $d_1,\ldots,d_m$ entiers et on construit un polynôme $P \in \mathbf{Z}[X_1\ldots,X_m]$ de degré au plus d_i en X_i, s'annulant beaucoup en $(\alpha,\ldots,\alpha)$ et dont les coefficients sont de taille controlée (Lemme de Siegel ou principe des boites).
Deuxième pas: On suppose qu'il existe $p_1/q_1,\ldots,p_m/q_m$ vérifiant (*); alors on prouve que P et un certain nombre de ses dérivées sont petits en

$\beta=(p_1/q_1,..,p_m/q_m)$ par une simple application de la formule de Taylor.

Troisième pas (difficile): On emploie un théorème de non-annulation, dont je donne ci-après un enoncé ("lemme de Roth à deux variables"). On doit prouver qu'une dérivée d'ordre assez petit est non nulle i.e.:

$\eta := \partial_i P(\beta) \neq 0$ avec $\partial_i = \frac{1}{i_1!..i_m!}(\partial/\partial X_1)^{i_1}..(\partial/\partial X_m)^{i_m}$.

Quatrième pas: comme η est rationnel et non nul on écrit :

$$(\text{Dénominateur}(\eta))^{-1} < |\eta|$$

C'est l''inégalité de Liouville"; elle fournit une contradiction si m est assez grand et si les q_i sont très échelonnés (Cf remarques ci-dessous)

Remarques:

i)Il est vital pour les estimations arithmétiques de diviser par les factorielles.

ii)Les théorèmes d'annulation (Dyson, Roth [Ro], Viola [Vi], Esnault-Viehweg [E–V]) utilisent la notion d'indice, ou ordre d'annulation pondéré; on définit l'indice d'un polynôme P en un point β par rapport aux poids $(d_1,...,d_m)$ par:

$$\text{Indice}_{(d_1,...,d_m)}(\beta)(P) := \min\{ \tfrac{i_1}{d_1}+..+\tfrac{i_m}{d_m} \ / \partial_i P(\beta)\neq 0\}.$$

Dans la pratique les d_i sont effectivement les degrés de P par rapport à X_i. Donnons l'énoncé promis:

LEMME DE ROTH ("À DEUX VARIABLES"): *soit* $\varepsilon>0$, α_1,α_2 *deux nombres algébriques et* $P\in \mathbb{Q}[X,Y]$ *non nul de degré au plus* d_1,d_2 *et supposons que*

1) $d_2/d_1<\varepsilon$

2) $h(P)+4d_1<\varepsilon^2\min(d_1h(\alpha_1),d_2h(\alpha_2))$

alors on a :

$$\text{Indice}_{(d_1,d_2)}(\alpha_1,\alpha_2)(P)<4\varepsilon.$$

Ici, h désigne la hauteur logarithmique usuelle (Cf paragraphe suivant). On pourra lire la preuve dans l'article original de Roth [Ro] ou dans celui de Bombieri [B]; il faut penser pour que le lemme soit utile que ε est petit et donc que d_1 est beaucoup plus grand que d_2 d'après (1) et donc pour majorer efficacement les dérivées de P (deuxième étape) et vérifier l'hypothèse (2) on aura besoin que $d_1h(\alpha_1)$ soit du

même ordre de grandeur que $d_2h(\alpha_2)$ et il faudra supposer:

(**) $h(\alpha_1)/h(\alpha_2) < \varepsilon$ ou encore $\log q_i/\log q_{i+1} < \varepsilon$

(avec les notations de la construction précédente) .

Ceci est la raison de l'ineffectivité congénitale de la méthode: on doit supposer l'existence de bonnes approximations avec des dénominateurs croissant exponentiellement pour montrer que de telles approximations n'existent pas. La preuve de Vojta souffre du même défaut et -tout comme la preuve de Faltings mais pour d'autres raisons- n'est pas effective. Par contre la méthode est très bonne pour borner le nombre des solutions (Cf théorème 2).

b) Jacobienne d'une courbe algébrique.

On définit un plongement de C dans une variété abélienne A=Jac(C) en choisissant un point origine $O \in C$. Sur $\mathbf{C}$ on procède ainsi: on choisit une base $\omega_1,..,\omega_g$ des 1–formes holomorphes sur C et on définit:

$j: C \longrightarrow A=Jac(C)=\mathbf{C}^g/\Omega$

$x \longrightarrow (\int_o^x \omega_1,..,\int_o^x \omega_g)$ modulo périodes.

Cette construction peut se faire algébriquement d'après Weil [W] (voir aussi l'article de Milne dans [Co-Si]). Dans ce cas A est une variété abélienne définie sur k et A(k) est un groupe de type fini. En particulier $A(k)\otimes\mathbf{R}=\mathbf{R}^r$ avec r=rangA(k) et l'application de C(k) dans cet espace est à fibres finies ("finite-to-one"). Ainsi pour prouver que C(k) est fini il suffit de prouver que son image dans $A(k)\otimes\mathbf{R}$ est finie.

Remarque: la description analytique donnée ci-dessus se transcrit mot pour mot à une variété X de dimension quelconque; on obtient ainsi une variété abélienne: sa variété d'Albanese (voir [La2]), mais bien sûr l'application obtenue n'est pas injective en général; en fait cela donne un caractérisation différentielle des sous-variétés de variétés abéliennes: ce sont celles qui ont "suffisamment" de 1-formes régulières.

2 Hauteurs associées à un diviseur.

C'est l'outil de base pour ces questions, des références générales sont [La1], [Se] et [Sz1]; en voici deux définitions donnant des éclairages différents: