Inégalités diophantiennes

Manuel Pégourié-Gonnard

Exposé du 14 mars 2007 au GTÉTN* de Bordeaux
Notes† du 23 mars 2007

Introduction : la géométrie diophantienne

Un des problèmes arithmétiques les plus anciens, et toujours d'actualité, est l'étude des équations (ou systèmes d'équations) diophantiennes, c'est-à-dire la recherche des solutions entières de systèmes d'équations polynomiales. La géométrie diophantienne consiste à essayer de comprendre le comportement de tels systèmes en utilisant les puissants outils de la géométrie algébrique. En effet, les objets historiquement étudiés sont :

- équations diophantiennes : les solutions $x \in \mathbf{Z}^n$ de systèmes $P_1(x) = \cdots = P_r(x) = 0$ avec $P_i \in \mathbf{Z}[X]$,
- variétés complexes (affines) : les points $x \in \mathbf{C}^n$ satisfaisant $P_1(x) = \cdots = P_r(x) = 0$ avec $P_i \in \mathbf{C}[X]$.

La ressemblance des objets est frappante, même si les différences sont manifestes : on a dans le deuxième cas (cas géométrique) un critère (constructif si l'on veut) d'existence de points complexes, fourni par le théorème des zéros de Hilbert. À l'inverse, un célèbre théorème de Matiyasevich implique qu'il n'existe pas d'algorithme décidant en temps fini de l'existence de solutions entières à une équation diophantienne de degré et nombre de variables arbitraires (répondant ainsi négativement au 10^{e} problème de Hilbert).

Introduisons un peu de vocabulaire. Pour $\boldsymbol{k}$ un corps, on dit qu'une sous-variété algébrique de l'espace affine (resp. projectif) est *définie sur* $\boldsymbol{k}$ si elle admet des équations formées de polynômes (resp. polynômes homogènes) à coefficients dans $\boldsymbol{k}$. De même, on dira d'un point qu'il est $\boldsymbol{k}$*-rationnel* s'il admet un système de coordonnées dans $\boldsymbol{k}$. Pour une variété V, on notera $V(\boldsymbol{k})$ l'ensemble de ses points $\boldsymbol{k}$-rationnels.

On a, de façon similaire, une notion de morphisme (ou d'application rationnelle) *défini sur* $\boldsymbol{k}$. Remarquons tout de suite que l'image d'un point

*Groupe de travail des étudiants en théorie des nombres. C'est avec plaisir que je remercie Fabien Pazuki pour l'invitation et les doctorants bordelais pour leur accueil.

†Parfois plus complètes ou détaillées que l'exposé oral.

$\boldsymbol{k}$-rationnel par une application rationnelle (*a fortiori* par un morphisme) définie sur $\boldsymbol{k}$ reste un point $\boldsymbol{k}$-rationnel.

Par ailleurs, regardons, par exemple, l'équation de FERMAT $x^n+y^n = z^n$, dont on cherche les solutions entières non triviales (en particulier, non identiquement nulles). L'équation étant homogène, toute solution dans $\mathbf{Q}^3$ en fournit une dans $\mathbf{Z}^3$ (et bien sûr réciproquement). En termes géométriques, la résolution du problème de FERMAT revient donc à comprendre tous les points $\mathbf{Q}$-rationnels de la courbe F_n définie par $x^n + y^n = z^n$ dans le plan projectif $\mathbf{P}^2$.

En simplifiant quelque peu, on peut donc dire que le problème initial des équations diophantiennes se traduit, en termes modernes, par la recherche des points $\mathbf{Q}$-rationnels (ou plus généralement $\boldsymbol{k}$-rationnels, où $\boldsymbol{k}$ est un corps de nombres) sur les variétés projectives. Un slogan de la géométrie diophantienne prédit que « la géométrie gouverne l'arithmétique », au moins dans un sens qualitatif (finitude ou non de l'ensemble des points rationnels, sur des corps de nombres assez gros).

Le but de cet exposé est, dans un premier temps, de montrer comment cette prédiction se réalise dans le cas des courbes, depuis la preuve par FALTINGS de la conjecture de MORDELL. Dans un second temps, nous introduirons quelques idées et outils (hauteurs) standards en géométrie diophantienne. Nous énoncerons enfin les inégalités de MUMFORD et de VOJTA, et verrons comment elles impliquent ensemble une version quantitative, mais pas effective, de l'ex-conjecture de MORDELL.

1 Classification diophantienne des courbes

1.1 Genre d'une courbe

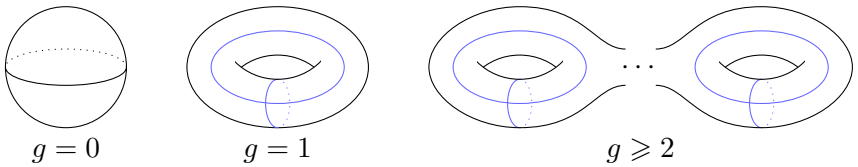
Soit C une courbe (irréductible), définie sur un corps de nombres K. Si $\boldsymbol{k}$ est une extension finie de K, on s'intéresse à la finitude de $C(\boldsymbol{k})$. La théorie générale des courbes algébriques montre que C est birationnellement équivalente à une courbe $\tilde{C}$ projective lisse (plongée dans $\mathbf{P}^3$ si l'on veut). L'application birationnelle peut être définie sur K si l'on veut, et induit donc une quasi-bijection[1] entre $C(\boldsymbol{k})$ et $\tilde{C}(\boldsymbol{k})$. On supposera donc dans tous les énoncés suivants que C est irréductible, projective et lisse.

L'ensemble $C(\mathbf{C})$ des points complexes de C forme alors une surface de RIEMANN compacte. On sait que de tels objets sont homéomorphes à une des surfaces représentées sur la figure 1.

Le « nombre de trous » d'une surface comme ci-dessus (0 pour la sphère) est appelé son genre. On peut le définir, un peu plus précisément, comme la demi-dimension du premier espace d'homologie réelle de la surface (dont une

[1] On entend par là une bijection entre $C(\boldsymbol{k})$ privé d'un nombre fini de points et $\tilde{C}(\boldsymbol{k})$ également privé d'un nombre fini de points.

FIG. 1 – Classification des surfaces de RIEMANN par le genre



base (en bleu) est représentée sur la figure 1). Des définitions équivalentes et plus algébriques existent, par exemple en termes de polynôme de HILBERT. En particulier le genre est tout à fait calculable. Pour les courbes planes sans singularités trop moches, la formule de RIEMANN-HURWITZ permet de calculer le genre en fonction du degré et du nombre de points doubles.

Nous allons voir ci-dessous que le genre, invariant purement géométrique, est une information suffisante pour comprendre qualitativement l'arithmétique d'une courbe. Signalons que le candidat éventuellement naturel que serait le degré n'est pas satisfaisant : en effet, la courbe $y^2 = x^5 + x^4$ possède une infinité de points $\mathbf{Q}$-rationnels, alors que $y^2 = x^5 + x$, de même degré, ne possède qu'un nombre fini de points rationnels sur $\mathbf{Q}$, et en fait sur tout corps de nombres.

Mentionnons, sans s'étendre sur le sujet, une autre manière de lire la classification des courbes. Utilisant les notions de classe canonique et d'amplitude des diviseurs, on a le découpage suivant, où K_C désigne la classe canonique :

- $g = 0 \Leftrightarrow -K_C$ est ample,
- $g = 1 \Leftrightarrow K_C = 0$,
- $g \leqslant 2 \Leftrightarrow K_C$ est ample,

qui permet d'étendre la classification aux variétés de dimension supérieure.

1.2 Courbes de genre 0

Les points complexes d'une courbe de genre 0 sont isomorphes (en tant que surface de RIEMANN) à la sphère de RIEMANN $\mathbf{P}^1(\mathbf{C})$ par définition. Des arguments formels montrent que cet isomorphisme provient d'un isomorphisme de variétés algébriques $C \approx \mathbf{P}^1$, qui est en fait défini sur $\overline{\mathbf{Q}}$, c'est-à-dire sur un corps de nombres L non précisé. Deux cas se présentent alors :

1. Si $\boldsymbol{k} \supset L$, on a $C(\boldsymbol{k}) = \mathbf{P}^1(\boldsymbol{k}) = \boldsymbol{k} \cup \{\infty\}$, qui est infini.
2. Sinon, $C(\boldsymbol{k}) = \emptyset$, mais il existe une extension finie de $\boldsymbol{k}$ sur laquelle C possède une infinité de points rationnels (cas précédent).

On peut observer cette dichotomie sur les exemples suivants. La courbe $x^2+y^2=z^2$ de $\mathbf{P}^2$ possède une infinité de points rationnels sur $\mathbf{Q}$ (donc sur tout corps de nombres) dont on peut donner une paramétrisation explicite par les points de $\mathbf{P}^1$. À l'inverse, la courbe $x^2+y^2=z^2$, elle aussi de genre 0, n'a pas de points rationnels sur $\mathbf{Q}$, mais en présente une infinité sur tout corps de nombres contenant i.

Ainsi, sur les corps de nombres assez grands, les courbes de genre 0 ont une infinité de points rationnels.

1.3 Courbes de genre 1

À défaut d'être le cas le plus simple, c'est certainement le plus connu : les courbes de 1 sont bien évidemment les courbes elliptiques. En tant que variétés complexes, elles sont le quotient $\mathbf{C}/(\mathbf{Z}\oplus\tau\mathbf{Z})$ de $\mathbf{C}$ par un réseau, ce qui les munit d'une loi de groupe commutatif. Il est bien connu que cette loi de groupe est en fait algébrique, et que les courbes elliptiques sont exactement les variétés abéliennes de dimension 1. Dans cette sous-section, on notera $E=C$. Le théorème de Mordell-Weil précise la structure de $E(\boldsymbol{k})$.

Théorème 1. *Soient E une courbe elliptique et $\boldsymbol{k}$ un corps de nombres contenant un corps de définition de E. Alors, soit $E(\boldsymbol{k})$ est vide, soit c'est un groupe de type fini. On a alors $E(\boldsymbol{k})\approx E(\boldsymbol{k})_{tor}\oplus\mathbf{Z}^r$, où r est par définition le rang de E sur $\boldsymbol{k}$.*

Ce théorème ne clôt néanmoins pas à lui seul la question de la finitude. En effet, il n'est pas clair *a priori* qu'il existe un corps de nombres sur lequel le rang soit non nul. Nous verrons tout à l'heure comment la théorie des hauteurs normalisées prouve que c'est pourtant le cas. Ainsi, la situation des courbes de genre 1 est semblable à celle des courbes de genre 0 : elles possèdent une infinité de points rationnels sur tout corps de nombres assez grand.

1.4 Courbes de genre 2 et plus

Le résultat suivant a été conjecturé par Mordell en 1922. Une première démonstration en a été obtenue par Faltings en 1983 et lui a valu une médaille Fields. Une démonstration indépendante, basée sur des idées plus traditionnelles d'approximation diophantienne, a été donnée par Vojta en 1990. Cette approche s'est montrée fructueuse et a permis la démonstration de la conjecture de Mordell-Lang par Faltings la même année, et ultérieurement de versions quantitatives totalement explicites (travaux de Bombieri, De Diego, Rémond). C'est l'approche que nous présenterons après avoir introduit les notions de hauteurs nécessaires. Contentons-nous pour l'instant d'énoncer le résultat de Faltings.

Théorème 2. *Soient C une courbe irréductible, projective, lisse, de genre g, et $\boldsymbol{k}$ un corps de nombres sur lequel C est définie. Si $g \geqslant 2$, $C(\boldsymbol{k})$ est fini.*

2 Notions de théorie des hauteurs

2.1 Hauteur projective

On commence par définir une notion de hauteur pour les points de l'espace projectif. La hauteur d'un point a pour fonction de mesurer sa complexité arithmétique, en un certain sens. Pour les points $\mathbf{Q}$-rationnels de l'espace projectif, c'est assez facile. Chaque $x \in \mathbf{P}^n(\mathbf{Q})$ admet un représentant $(x_0, \ldots, x_n)$ tel que les x_i soient des entiers premiers entre eux. On pose alors $H(x) = \max(|x_0|, \ldots, |x_n|)$. On utilisera courament la hauteur logarithmique $h = \log H$.

Cette dernière représente, de façon fort concrète, le nombre de bits sur lequel il faut représenter les entiers dans un système informatique pour pouvoir y décrire x. De façon équivalente, on peut la regarder comme la quantité d'information contenue dans x. On a donc bien affaire à une mesure de complexité.

On généralise la hauteur aux corps plus gros que $\mathbf{Q}$ de la façon suivante :

$$h(x) = \sum_{v \in M(\boldsymbol{k})} \frac{[\boldsymbol{k}_v : \mathbf{Q}_v]}{[\boldsymbol{k} : \mathbf{Q}]} \log \max(|x_0|_v, \ldots, |x_n|_v) \ ,$$

où $\boldsymbol{k}$ est un corps tel que $x \in \mathbf{P}^n(\boldsymbol{k})$ et $M(\boldsymbol{k})$ l'ensemble de ses valeurs absolues. Deux mots sur les normalisations : on choisit les valeurs absolues de $\boldsymbol{k}$ qui prolongent les valeurs absolues de $\mathbf{Q}$. Le coefficient $[\boldsymbol{k}_v : \mathbf{Q}_v]$ est alors celui qui apparaît dans la formule du produit, ce qui assure que la hauteur est bien définie et ne dépend pas du représentant $(x_0, \ldots, x_n)$ choisi. Par ailleurs, il n'est pas très difficile de vérifier que, grâce au facteur $\frac{1}{[\boldsymbol{k}:\mathbf{Q}]}$, le résultat ne dépend pas non plus du corps de nombres $\boldsymbol{k}$ dans lequel on fait le calcul. On a donc bien prolongé la hauteur projective en une fonction $\mathbf{P}^n(\mathbf{Q}) \to \mathbf{R}$.

La hauteur ainsi définie possède deux propriétés fondamentales et très intéressantes. La première est d'être bornée inférieurement ; en fait, la hauteur définie ci-dessus est positive par la formule du produit. La seconde est une propriété de finitude : l'ensemble des points de hauteur bornée définis sur un corps de nombres donné est fini. Ce résultat est trivial sur $\mathbf{Q}$: il provient du fait qu'on a qu'un nombre fini de choix possibles pour les coordonnées. Il n'est pas difficile de l'étendre à un corps de nombres *via* la notion de polynôme minimal, une fois qu'on a établi que la hauteur d'un nombre se reflète sur celle de son polynôme minimal. On obtient même le résultat plus précis suivant :

Théorème 3. *Soient d et B deux entiers naturels. L'ensemble*

$$\{x \in \mathbf{P}^n(\boldsymbol{k}) \text{ où } [\boldsymbol{k} : \mathbf{Q}] \leqslant d \text{ et } h(x) \leqslant B\}$$

est fini.

L'usage veut[2] qu'on attribue ce théorème à NORTHCOTT même s'il était sans doute connu d'autres personnes. Le résultat devient par contre faux si l'on enlève la borne sur le degré de $\boldsymbol{k}$.

2.2 Hauteur sur les variétés

La théorie des hauteurs sur les variétés est sans doute la partie la plus intéressante. En effet, les différentes fonctions de hauteur qu'on peut définir sur une variété reflètent de façon assez profonde la géométrie de cette dernière. C'est ce qui permet à la hauteur de jouer le rôle de passerelle entre la géométrie et l'arithmétique, et justifie son rôle central en géométrie diophantienne. Faute de temps, et pour garder l'exposé accessible sans connaissances de la théorie des diviseurs, je n'approfondirai pas beaucoup cet aspect pourtant fondamental.

Disons cependant qu'on peut définir une hauteur h_ϕ sur une variété V dès qu'on s'est fixé un morphisme $\phi : V \to \mathbf{P}^n$, par la formule naturelle $h_\phi = h \circ \phi$. Bien qu'un morphisme quelconque suffise, dans la pratique on considérera souvent des immersions[3] (fermées ou non), afin de conserver la propriété de finitude énoncée plus haut. La hauteur ainsi définie dépend bien évidemment de ϕ. C'est dans cette dépendance en ϕ que se cachent les aspects géométriques de la théorie des hauteurs, que nous n'approfondirons donc pas.

Par exemple, on peut attribuer une hauteur aux nombres *via* l'immersion ouverte évidente $\mathbf{A}^1 \hookrightarrow \mathbf{P}^1$. On obtient ainsi la formule naturelle $H(a/b) = \max(|a|, |b|)$ pour la hauteur des nombres rationnels. Dans le cas de la droite affine, on retrouve même sur la hauteur des propriétés agréables comme $H(x + y) \leqslant H(x) + H(y)$, qui découle de l'inégalité triangulaire appliquée en chaque place. On s'attend, de façon générale, à ce que la hauteur sur les groupes algébriques ait un comportement agréable vis-à-vis de la loi de groupe.

Regardons le cas du groupe multiplicatif $\mathbf{G}_m$. On a évidement $h(xy) \leqslant h(x)h(y)$ (on vérifie l'inégalité terme à terme). On n'a par contre pas d'inégalité en sens contraire, sauf l'inégalité triviale $h(xy) \geqslant 0$ (exemple : $x = 1/2$ et $y = 2$). On a toutefois des propriétés plus précises pour l'exponentiation : $h(x^m) = |m| h(x)$ pour tout m entier. Une autre propriété intéressante est

[2] En fait, l'usage veut aussi que l'on précise que l'attribution du théorème à NORTHCOTT n'est due qu'à l'usage...

[3] Plus précisément, si V est projective, il suffit que le fibré associé à ϕ soit ample pour conserver la propriété de finitude.

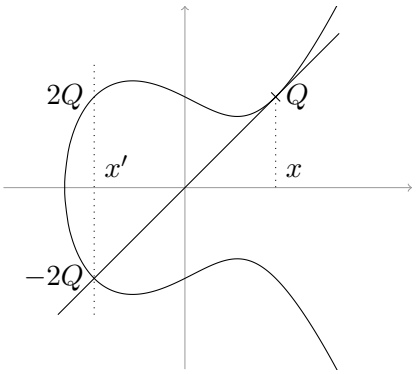
la caractérisation des points de torsion (ici, les racines de l'unité) par l'annulation de la hauteur : $h(x) = 0$ si et seulement si x est racine de l'unité.

2.3 Hauteurs normalisées

Regardons maintenant ce qui se passe sur les groupes algébriques particulièrement intéressants que sont les variétés abéliennes, en commençant par le cas de dimension 1 : les courbes elliptiques.

On considère une courbe elliptique E plongée dans le plan avec une équation du type $Y^2 = P(X)$ (pour sa partie affine), où P est un polynôme séparable de degré 3. On sait que dans un tel plongement, la loi d'addition se lit naturellement sur la courbe, en particulier la multiplication par deux se lit géométriquement, comme représenté sur la figure 2.

FIG. 2 – Multiplication par 2 sur une courbe elliptique



Étudions l'action de la multiplication par deux sur la hauteur. Soit $Q = (x, y)$ un point de la courbe (on suppose $P(x) \neq 0$ pour simplifier). Comme y est algébriquement lié à x par le polynôme P, sa contribution à la hauteur de Q est comparable à celle de x ; pour contrôler (à constante près) la hauteur de Q, il suffit donc de contrôler $h(x)$. Notons (x', y') les coordonnées de $2Q$, et calculons x' en fonction de x.

On écrit d'abord que Q et $2Q$ sont sur la tangente à E en Q :

$$y' - y = \frac{P'(x)}{2y}(x' - x) \ ,$$

puis que les deux sont également sur E :

$$P(x') = \left(\frac{P'(x)}{2y}(x' - x) + y\right)^2 = \frac{P'(x)^2}{4P(x)}(x' - x)^2 + P'(x)(x' - x) + P(x) \ .$$

On utilise alors un développement de TAYLOR :

$$\frac{P'(x)^2}{4P(x)} = \frac{\frac{P(x')-P(x)}{x'-x} - P'(x)}{x' - x} = \frac{1}{2}P''(x) + \frac{1}{6}P'''(x)(x' - x) \ ,$$

et finalement :

$$x' = x + \frac{6}{P'''(x)}\left(\frac{P'(x)^2 - 2P(x)P''(x)}{4P(x)}\right) = \frac{R(x)}{S(x)}\ ,$$

où R et S sont des polynômes de degré respectifs 4 et 3 ne dépendant que de E.

Il est alors facile de vérifier à l'aide de l'inégalité triangulaire que $h(x') \leqslant 4h(x) + c_1$, où c_1 est une constante ne dépendant que de E, explicite[4] si l'on veut. Il est un peu plus difficile, mais guère plus, de prouver l'inégalité inverse : $h(x') \geqslant 4h(x) - c_2$, où c_2 est une autre constante[5] positive.

On constate donc un comportement proche de celui constaté sur le groupe multiplicatif, mais cette fois quadratique, et surtout « à constante près ». Ce dernier point étant fort déplaisant, on utilise un mécanisme de normalisation, dont la théorie générale est due à Néron et Tate, qui est ici fort simple. On vérifie aisément que la limite en l'infini de $h(2^nQ)/4^n$ existe. On la note $\hat{h}(Q)$ et on l'appelle *hauteur normalisée* (ou de Néron-Tate) de Q.

Il est immédiat que $\hat{h}(2Q) = 4\hat{h}(Q)$ (c'est fait pour !), et que $|\hat{h} - h| \leqslant c_3$. Ce point est important, notament parce qu'il permet à $\hat{h}$ d'hériter des propriétés de finitude de h. On peut montrer par ailleurs que pour tout entier m, on a $\big|h(mQ) - m^2h(Q)\big| \leqslant c(m)$. On en déduit alors aisément que $\hat{h}(mQ) = m^2h(Q)$, ce qui est réjouissant. On retrouve ainsi la même caractérisation des points de torsion, comme points de hauteur nulle, que dans le cas du groupe multiplicatif. En effet,

$$\begin{aligned} Q \text{ de torsion } &\Leftrightarrow \{2^nQ\}_{n\in\mathbf{N}} \text{ est fini} \\ &\Leftrightarrow \{\hat{h}(2^nQ)\}_{n\in\mathbf{N}} \text{ est borné} \\ &\Leftrightarrow \{4^n\hat{h}(Q)\}_{n\in\mathbf{N}} \text{ est borné} \\ &\Leftrightarrow \hat{h}(Q) = 0\ . \end{aligned}$$

On constate que ceci permet, si l'on ne connaissait pas déjà le théorème de Mordell-Weil, de redémontrer la finitude de $E(\boldsymbol{k})_{\text{tor}}$: c'est en effet un ensemble de hauteur normalisée bornée, car nulle ! Le fait que la constante de comparaison entre $\hat{h}$ et h dépende de E interdit par contre d'espérer en tirer des bornes uniformes sur la torsion, telles que fournies par le théorème de Merel.

De plus, on peut répondre à la question posée tout à l'heure de savoir si le rang de $E(\overline{\mathbf{Q}})$ est non nul. On peut construire sur $\overline{\mathbf{Q}}$ des points de E

[4] On peut prendre $c_1 = h(R,S) + \log\max(\mathcal{N}(R),\mathcal{N}(S))$, où $h(R,S)$ est la hauteur du vecteur formé des coefficients de R et de S, et $\mathcal{N}(\,\cdot\,)$ désigne le nombre de coefficients (exercice si l'on veut).

[5] Il est également possible de donner une valeur explicite à cette constante, mais cela nécessite de disposer d'une version effective du théorème des zéros de Hilbert. Le calcul de c_2 n'est donc pas laissé en exercice...

de hauteur projective arbitrairement grande. En effet, si p est un nombre premier assez grand[6] on vérifie sans peine que le point Q de coordonnées $(p, \sqrt{P(p)})$ est de hauteur au moins p. Un tel point vérifie alors $\hat{h}(Q) > 0$, et est donc d'ordre infini. Ainsi, sur tout corps de nombres assez grand (pour que Q soit y soit rationnel), E a une infinité de points rationnels comme annoncé en 1.2.

Après ce début de construction assez détaillé, je demande au public d'admettre les faits suivants :

- Non seulement $\hat{h}$ est homogène de degré 2, mais c'est en fait une vraie forme quadratique. (On peut vérifier par un calcul explicite que h satisfait l'égalité du parallélogramme à constante près, et en déduire que $\hat{h}$ la satisfait pour de vrai.)
- Cette forme quadratique se prolonge en une forme quadratique définie positive sur $E(\overline{\mathbf{Q}}) \otimes_{\mathbf{Z}} \mathbf{R}$. (C'est réaliste, puisque la tensorisation par un corps tue la torsion, c'est-à-dire ici les vecteurs isotropes. On démontre par ailleurs qu'étendre les scalaires à $\mathbf{R}$ ne rajoute pas de cochonneries.)
- Tout ceci marche exactement de la même manière[7] sur une variété abélienne quelconque.

On a maintenant réuni le matériel nécessaire pour aborder la méthode de Vojta sur la conjecture de Mordell.

3 Inégalités de Mumford et de Vojta

Désormais C est une courbe de genre $g \geqslant 2$. Cela implique qu'il existe une variété abélienne A et un plongement $C \hookrightarrow A$. On peut par exemple prendre la jacobienne J de C, qui est alors de dimension g, munie d'un plongement $\iota : C \hookrightarrow J$ donné par $\iota(P) = [P - P_0]$, où P_0 est un point fixé de C, et $[P - P_0]$ désigne la classe du diviseur $P - P_0$ (on rappelle que les poins de la jacobienne sont les classes de diviseurs de degré 0 de C). Comme $g \neq 1$, C n'est pas isomorphe à une sous-variété abélienne de J (en effet les courbes elliptiques sont les seules variétés abéliennes de dimension 1), en particulier son stabilisateur[8] est fini. Il est remarquable que ce fait, ainsi que l'existence d'un plongement $C \hookrightarrow J$, est le seul endroit dans la preuve où intervient l'hypothèse $g \geqslant 2$.

Regardons de plus près le plongement ι. Il est défini sur $\boldsymbol{k}$ si et seulement si P_0 est un point $\boldsymbol{k}$-rationnel. Deux cas se présentent alors : soit $C(\boldsymbol{k})$ est

[6] Par exemple, plus grand que tous les facteurs premiers de g_3 si l'équation de E et $y^2 = 4x^3 - g_2x - g_3$, de sorte que p et $P(p)$ sont premiers entre eux.

[7] Il faut quand même préciser que cela dépend du plongement projectif choisi au départ pour définir h. En fait, $\hat{h}$ ne sera une forme quadratique que si le fibré associé au plongement est « symétrique ». C'est un exemple intéressant de l'interaction géométrie-hauteur évoquée plus haut. On suppose dans toute la suite que $\hat{h}$ est quadratique.

[8] On regarde J comme agissant sur elle-même par translation.

vide, et il n'est pas difficile de prouver qu'il est fini, soit on peut choisir P_0 tel que ι est défini sur $\boldsymbol{k}$. On a alors une injection $C(\boldsymbol{k}) \hookrightarrow J(\boldsymbol{k})$. L'application composée $C(\boldsymbol{k}) \hookrightarrow J(\boldsymbol{k}) \to J(\boldsymbol{k}) \otimes_{\mathbf{Z}} \mathbf{R}$ est alors à fibres finies (le noyau du deuxième morphisme étant la torsion, qui est finie). Pour prouver la finitude de $C(\boldsymbol{k})$, il suffit donc de prouver celle de son image dans $J(\boldsymbol{k}) \otimes_{\mathbf{Z}} \mathbf{R}$. Cette dernière est une conséquence de l'énoncé suivant :

Théorème 4 (Inégalité de Vojta (IV), 1990)**.** *Sous les hypothèses précédentes, il existe des constantes $\alpha > 0$, β et γ telles que, pour tous points x et y de $C(\overline{\mathbf{Q}})$, les trois conditions suivantes sont incompatibles :*

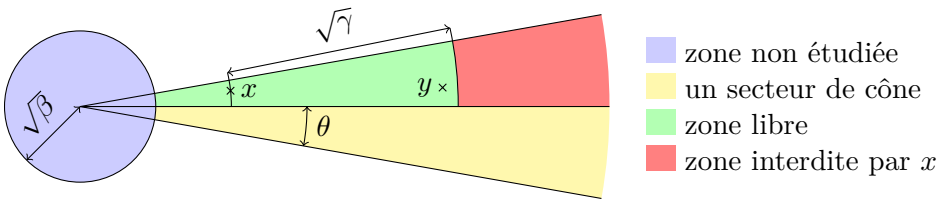
1. $\hat{h}(x) \geqslant \beta$,
2. $\cos(x, y) \geqslant 1 - \alpha$,
3. $\hat{h}(y) \geqslant \gamma \hat{h}(x)$.

Cet énoncé appelle un certain nombre de commentaires. Des valeurs convenables des constantes ont été explicitement calculées, et ne dépendent que du genre de C et de la hauteur[9] de sa jacobienne. Je ne donne pas les valeurs qui sont assez « techniques », et dont il n'est pas très facile de savoir quelle version est la meilleure.

Par ailleurs, on a (un peu abusivement) confondu les points de C et leur image dans $J(\overline{\mathbf{Q}}) \otimes_{\mathbf{Z}} \mathbf{R}$, ce qu'on fera systématiquement dans la suite. Le cos fait référence à la structure euclidienne de $J(\overline{\mathbf{Q}}) \otimes_{\mathbf{Z}} \mathbf{R}$ donnée par la forme quadratique $\hat{h}$. Enfin, la première condition n'est pas restrictive, puisqu'elle n'exclut qu'un nombre fini de points.

Les trois conditions ont une interprétation géométrique simple : la première demande que x soit à l'extérieur d'une boule de rayon $\sqrt{\beta}$ centrée en l'origine ; la deuxième, que les deux points se trouvent dans un même secteur de cône d'angle $\theta = \arccos(1-\alpha)$. Si ces deux conditions sont remplies, alors y ne peut pas être de hauteur trop grande, comme illustré sur la figure 3.

Fig. 3 – Inégalité de Vojta



Ainsi, pour chaque secteur de cône tronqué S, deux possibilités se présentent : soit S ne contient aucun point de C, et c'est très bien, soit $C(\overline{\mathbf{Q}}) \cap S$

[9] Nous n'avons pas défini ici de notion de hauteur pour les variétés. Une telle hauteur peut pourtant être définie, de différentes manières. Pour les variétés abéliennes, citons notamment la hauteurs de Faltings et celle définie *via* les *thetanullwerte*.

est borné, ce qui est aussi plaisant. En effet, $J(\boldsymbol{k}) \otimes_{\mathbf{Z}} \mathbf{R} \approx \mathbf{R}^r$ est de dimension finie (par le théorème de Mordell-Weil, et peut donc être recouvert par un nombre fini de secteurs de cônes (on a utilisé le fait que $\boldsymbol{k}$ est un corps de nombres). Ainsi, l'image de $C(\boldsymbol{k})$, qui est contenue dans une réunion finie d'ensemble de hauteur bornée, est de hauteur bornée (on utilise à nouveau que $\boldsymbol{k}$ est de degré fini). Vu la propriété fondamentale de la hauteur, cela implique que $C(\boldsymbol{k})$ est fini.

On vient de voir que l'inégalité de Vojta implique la conjecture de Mordell. En fait, elle est nettement plus précise comme va l'illustrer la suite (conjonction avec l'inégalité de Mumford). Signalons tout de suite un point remarquable : l'inégalité est valable sur $\overline{\mathbf{Q}}$, et ce n'est que dans l'implication (IV) $\Rightarrow$ Mordell qu'intervient $\boldsymbol{k}$. Cela permet par exemple de prouver que le rang de J sur $\overline{\mathbf{Q}}$ est infini : en effet, dans le cas contraire, la première partie du raisonnement ci-dessus s'appliquerait, prouvant que $C(\overline{\mathbf{Q}})$ est de hauteur bornée, ce qui est visiblement faux.

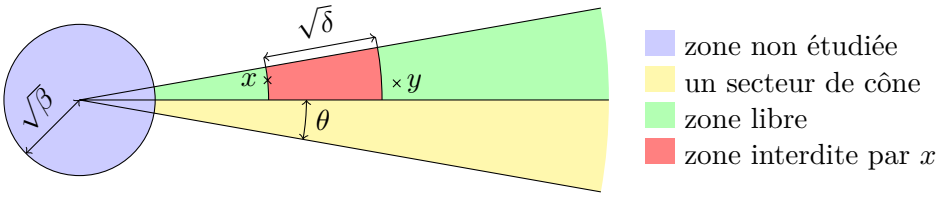
L'inégalité de Mumford a été prouvée, bien qu'énoncée sous une autre forme, en 1965. Sous la forme suivante, sa ressemblance avec l'inégalité de Vojta est claire.

Théorème 5 (Inégalité de Mumford (IM), 1965)**.** *Sous les hypothèses précédentes, il existe des constantes $\alpha > 0$, β et δ telles que, pour tous points x et y de $C(\overline{\mathbf{Q}})$ (distincts modulo le stabilisateur de C dans J), les trois conditions suivantes sont incompatibles :*

1. $\hat{h}(x) \geqslant \beta$,
2. $\cos(x, y) \geqslant 1 - \alpha$,
3. $\hat{h}(x) \leqslant \hat{h}(y) \leqslant \delta \hat{h}(x)$.

Comme pour (IV), les constantes peuvent être choisies de façon explicite. La seule différence, hormis l'hypothèse technique concernant le stabilisateur, est dans la dernière condition, qui cette fois demande que les points soient de hauteur voisine et non plus très différente. La conclusion géométrique est donc cette fois qu'il existe une « zone d'exclusion » autour de chaque point de hauteur assez grande, comme illustré sur la figure 4.

Fig. 4 – Inégalité de Mumford



Seule, l'inégalité de Mumford implique le théorème de Mumford, sur la fonction de comptage des courbes de genre 2 ou plus. On définit la fonction

de comptage par $N(C, \boldsymbol{k}, B) = \mathrm{Card}\{x \in C(\boldsymbol{k}) \text{ tel que } h(x) \leqslant B\}$. On voit facilement que (IM) implique que dans chaque secteur de cône, la hauteur croît au moins exponentiellement. Par finitude du nombre de secteurs, on en déduit facilement le théorème de Mumford : $N(C, \boldsymbol{k}, B) = O(\log B)$.

Ce résultat, aujourd'hui rendu obsolète par le théorème de Faltings, était à l'époque un indice important pour croire à la conjecture de Mordell, dans le sens où les points rationnels sont « plus rares » sur les courbes de genre au moins 2 que sur celles de genre inférieur. En effet, on peut montrer que $N(\mathbf{P}^1, \boldsymbol{k}, B) \approx \exp 2B$ et $N(E, \boldsymbol{k}, B) \approx B^{r/2}$, où r désigne le rang de E sur $\boldsymbol{k}$.

Si le théorème de Mumford est obsolète, il n'en est pas de même de son inégalité. En effet, jointe à celle de Vojta, elle permet d'obtenir simplement une version quantitative du théorème de Faltings. Dans chaque secteur de cône tronqué, supposons qu'il existe une suite $x_1, \ldots, x_n$ de points de C distincts modulo le stabilisateur (qui est d'ordre majoré par $\deg(C)^2$). On peut leur appliquer les deux inégalités : $\delta^n \hat{h}(x_1) \leqslant \hat{h}(x_1) \leqslant \gamma(x_1)$, d'où $n \leqslant \log(\gamma/\delta)$. Comme on peut également compter le nombre de cônes suffisant à recouvrir l'espace, on en déduit un résultat de décompte, dont j'énonce ci-dessous une version due à Farhi, sans prétendre que ce soit la meilleure connue à ce jour.

Théorème 6. *Soit C une courbe (irréductible, projective, lisse) de genre $g \geqslant 2$. On note J sa jacobienne, r le rang de cette dernière sur $\boldsymbol{k}$, et $h(J)$ sa hauteur relative aux* thetanullwerte*, et enfin $h_0(J) = [\boldsymbol{k} : \mathbf{Q}] \max(1, h(J))$. Alors*

$$\mathrm{Card}\, C(\boldsymbol{k}) \leqslant 2^{82g^3} h_0(J)^{8g} \left[2^{43g^3} h_0(J)^{5g}\right]^r \quad .$$

Deux précisions sur ce résultat : les inégalités de Vojta et Mumford laissent de côté, comme nous l'avons vu, les points de hauteur petite. Il faut donc savoir compter assez précisément les points de petite hauteur sur une courbe, ce qui met en jeu des techniques raffinées dont je ne parlerai pas faute de compétences. Par ailleurs, certaines conjectures plus générales de Lang indiquent qu'on devrait pouvoir obtenir une majoration du nombres de points qui ne fasse pas intervenir la hauteur $h(J)$ de la jacobienne. De tels résultats ne sont aujourd'hui pas connus en général.

Par ailleurs, signalons le gros problème de la méthode de Vojta, malheureusement partagé par la plupart des méthodes diophantiennes connues : il s'agit du manque d'effectivité, c'est-à-dire de l'absence de borne explicite de la hauteur des points. En effet, on a montré dans chaque secteur de cône que la hauteur était bornée, mais la borne dépend de la hauteur du premier point existant dans ce secteur de cône tronqué. Or celle-ci peut être arbitrairement grande, et il paraît peu raisonnable d'espérer la contrôler.

Pourtant, connaître une borne de hauteur explicite serait extrêmement intéressant, car cela fournirait un moyen, au moins théorique, de trouver tous

les points rationnels de C : en effet, il n'est pas difficile d'énumérer tous les points de petite hauteur de l'espace projectif, et de vérifier un par un s'ils sont sur C. Même si un tel algorithme n'aurait sans doute aucune utilité pratique (complexité au moins exponentielle), le problème de l'effectivité reste très intéressant, et aujourd'hui extrêmement difficile. Signalons par exemple que certaines versions de Mordell effectif impliquent des versions de la conjecture *abc*.

Arrivé au terme de cet exposé, j'espère avoir donné un aperçu représentatif de la géométrie diophantienne : l'idée générale que la géométrie détermine l'arithmétique, un survol de l'outil fondamental qu'est la théorie des hauteurs, et enfin un résultat caractéristique des connaissances actuelles : une bonne compréhension qualitative, des résultats quantitatifs, mais le problème encore grand ouvert de l'effectivité.