

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Gaël RÉMOND

Borne polynomiale pour le nombre de points rationnels des courbes

Tome 23, n° 1 (2011), p. 251-255.

http://jtnb.cedram.org/item?id=JTNB_2011__23_1_251_0

© Société Arithmétique de Bordeaux, 2011, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

Borne polynomiale pour le nombre de points rationnels des courbes

par GAËL RÉMOND

RÉSUMÉ. Soit F un polynôme en deux variables, de degré D et à coefficients entiers dans $[-M, M]$ pour $M \geq 3$. Alors le nombre de zéros rationnels de F est soit infini soit plus petit que $M^{2^{3D^2}}$. Nous montrons aussi une version plus générale sur les corps de nombres.

ABSTRACT. *Polynomial bound for the number of rational points on curves.*

Let F be a polynomial in two variables with integer coefficients, D its degree and $M \geq 3$ an upper bound for the absolute value of its coefficients. Then the number of rational zeroes of F is either infinite or less than $M^{2^{3D^2}}$, a polynomial bound in M . We also give a more general statement for number fields. The proof is a variation on an earlier result together with an easy counting lemma for rational points.

1. Introduction

Le but de cette note est de borner le nombre de zéros rationnels d'un polynôme à coefficients entiers de manière polynomiale en ses coefficients.

Théorème 1. *Soit $F \in \mathbb{Z}[X, Y]$ de degré D et soit $M \geq 3$ un majorant de la valeur absolue des coefficients de F . Alors l'ensemble $\{(x, y) \in \mathbb{Q}^2 \mid F(x, y) = 0\}$ est ou bien infini ou bien de cardinal au plus $M^{2^{3D^2}}$.*

Le résultat précédent s'obtient en fait comme cas particulier d'un théorème sur les corps de nombres. Nous y utilisons la hauteur d'un polynôme (logarithmique, absolue et définie par des normes du supremum à l'infini). La notation $\Delta_{K/\mathbb{Q}}$ désigne le discriminant absolu d'un corps de nombres K .

Théorème 2. *Soient K un corps de nombres et $F \in K[X, Y]$ de degré D . Alors, si l'ensemble $\{(x, y) \in K^2 \mid F(x, y) = 0\}$ est fini, il est de cardinal au plus*

$$\exp\left(2^{3D^2} [K : \mathbb{Q}]^4 \max(h_\infty(F), \log |\Delta_{K/\mathbb{Q}}|, 1)\right).$$

Nous obtenons cette borne en modifiant légèrement l'approche de [R2]. Dans cet article précédent, nous démontrions le même énoncé avec la borne :

$$\exp\left(5^{D^4}[K:\mathbb{Q}]^5 \max(h_\infty(F), \log|\Delta_{K/\mathbb{Q}}|, 1) \log(h_\infty(F) + 2)\right).$$

Nous améliorons donc la dépendance en la hauteur (et très légèrement celle en le degré de K) au prix d'une perte assez sensible sur le terme de degré.

Les calculs de [R2] se basent sur le travail effectué dans [R1]. Pour compter les points rationnels d'une courbe de genre au moins deux, nous les séparons en deux ensembles : d'une part les grands points font l'objet de la méthode de Vojta-Faltings-Bombieri et il faut borner par ailleurs les petits points. Pour cela, dans [R1] et [R2], nous invoquons un théorème de Philippon et David sur le problème de Bogomolov (voir [DP]) qui permet de majorer assez finement le nombre de petits points.

De manière un peu plus précise, avec les notations du théorème 2 ci-dessus, la hauteur critique (celle qui sépare petits et grands points) se trouve être linéaire en $h(F)$. Par suite la borne de Philippon-David est polynomiale en $h(F)^r$ où r est le rang de la jacobienne sur K . Ceci semble à première vue polynomial en $h(F)$ donc encore meilleur que ce que l'on veut obtenir (exponentiel en $h(F)$). Malheureusement, les estimations connues pour le rang r (voir [R2]) sont elles-mêmes linéaires en $h(F)$ d'où la dépendance qui apparaît dans [R2]. Pour être complet, disons aussi que le nombre de grands points se borne en c^r pour une constante c ne comportant pas de termes de hauteur.

Ici, nous changeons le décompte des petits points. Au lieu du résultat fin de [DP], nous employons un décompte beaucoup plus élémentaire : nous majorons le nombre de points de hauteur bornée sur C par le nombre de points de hauteur bornée dans un espace projectif dans lequel C est plongée. La dépendance en la hauteur critique devient exponentielle au lieu de polynomiale mais le rang disparaît de l'estimation des petits points. Ainsi la borne finale est de la forme $\exp(c'h(F)) + c^r \leq \exp(c''h(F))$ pour diverses constantes c, c' et c'' indépendantes de la hauteur. La perte sur D provient de l'estimation de c' .

2. Décompte

Nous utiliserons l'effectivisation élémentaire suivante du théorème de Northcott.

Lemme 1. *Le nombre de points de $\mathbb{P}^n(\overline{\mathbb{Q}})$ de degré au plus D et de hauteur au plus H est majoré par $\exp((n+1)D^3(H+2))$.*

Démonstration. Dans un premier temps, nous associons à chaque point x concerné un $(n+1)$ -uplet (x_0, \dots, x_n) de coordonnées projectives formé

d'entiers algébriques tels que $h_\infty(1, x_0, \dots, x_n) \leq DH$ (voir lemme 5.1 de [R2]). Nous associons ensuite à chaque x_i son polynôme minimal $P_i \in \mathbb{Z}[X]$ de degré $D_i \leq D$ puis le polynôme $Q_i = X^{D-D_i}P_i$ unitaire de degré D . De cette façon, nous avons défini une application de notre ensemble vers $\mathbb{Z}^{(n+1)D}$ (qui envoie x sur les coefficients des Q_i). Chaque fibre de cette application contient au plus D^{n+1} points. D'autre part la valeur absolue d'un coefficient de Q_i (ou de P_i) est majorée de la manière suivante :

$$\left| \sum_{j_1 < \dots < j_k} \sigma_{j_1}(x_i) \cdots \sigma_{j_k}(x_i) \right| \leq \binom{D_i}{k} \prod_{v|\infty} \max(1, |x_i|_v^{n_v}) \leq 2^{D_i} e^{D_i h(x_i)}$$

où $1 \leq k \leq D_i$, la lettre v désigne une place de $K = \mathbb{Q}(x_i)$ et $n_v = [K_v : \mathbb{Q}_v]$ est le degré local tandis que les σ_j pour $1 \leq j \leq D_i$ sont les différents plongements de K dans \mathbb{C} . Par suite le nombre cherché est au plus

$$D^{n+1} (2^{D+1} e^{D^2 H} + 1)^{(n+1)D}$$

et cette quantité est facilement majorée par celle de l'énoncé. □

Nous nous référons maintenant à la deuxième partie du théorème 2.1 de [R1]. Dans les définitions qui le précèdent, si l'on utilise $\Gamma = A(K)$ alors on peut remplacer la fonction Ω qui comptait les petits points à la façon de [DP] par une expression tirée du lemme précédent. Plus précisément dans les notations de [R1] nous remplaçons

$$\Omega(r, 1, \deg X, c)$$

par

$$\exp((n+1)[K : \mathbb{Q}]^3 ((c+1) \max(1, c_{NT}, h_1) + 2))$$

(on note la disparition du rang r). Nous souhaitons maintenant procéder comme dans la proposition 10.1 de [R2] c'est-à-dire appliquer ceci à une courbe $C = X$ de genre $g \geq 2$ plongée dans sa jacobienne elle-même plongée dans \mathbb{P}^n avec $n = 2^{4g} - 1$ par un plongement thêta associé à (seize fois) un diviseur thêta symétrique de la jacobienne. Dans ce cadre, David et Philippon montrent $c_{NT} \leq 4^{g+1} h_\theta + 3g \log 2$ (proposition 3.9 de [DP]) et $h_1 \leq 2(4^g - 1) h_\theta$ (proposition 3.7) où h_θ est la hauteur thêta utilisée dans [R2]. En outre $\deg X = 16g$ donc la quantité D apparaissant dans le théorème 2.1 de [R1] vaut $\max(16g, 2^{14})$ que nous majorons par 2^{7g} . En combinant tout ceci, il vient

Card $C(K)$

$$\begin{aligned} &\leq \exp((n+1)2^{6g}[K : \mathbb{Q}]^3 (n+1)^2 D^{20} (2 + 3 \log(n+1)) \max(1, c_{NT}, h_1)) \\ &\quad + (3(n+1)^2 D^{12})^r \\ &\leq \exp(2^{4g} 2^{6g} [K : \mathbb{Q}]^3 2^{8g} 2^{140g} (11g)(4^{g+1} h_\theta + 3g)) + (3 \cdot 2^{8g} 2^{84g})^r \\ &\leq \exp(2^{164g} [K : \mathbb{Q}]^3 \max(1, h_\theta)) + 2^{94gr} \end{aligned}$$

où sur la première ligne nous avons remplacé $[K : \mathbb{Q}]$ par $2^{2g}[K : \mathbb{Q}]$ pour tenir compte de l'extension de corps éventuelle pour rendre le diviseur thêta symétrique.

3. Calculs

Il reste à reprendre les calculs de la dernière partie de [R2] à partir de la formule ci-dessus pour aboutir au théorème 2. Pour alléger, nous notons comme dans cet article $H_1 = \max(h_\infty(F), \log |\Delta_{K/\mathbb{Q}}|, 1)$.

Nous suivons d'abord la proposition 10.1. Dans le cas présent, nous devons montrer

$$\exp(2^{164g}[K : \mathbb{Q}]^3 \max(1, h_\theta)) + 2^{94gr} + D^2 \leq \exp(2^{3D^2}[K : \mathbb{Q}]^4 H_1).$$

La majoration de $r + 1$ qui figure dans [R2] entraîne d'une part $94gr \leq 5D^4 - 64[K : \mathbb{Q}]^4 H_1$ donc $2^{94gr} + D^2$ est inférieur à la moitié du majorant cherché. Pour h_θ , les calculs donnent

$$\begin{aligned} \max(1, h_\theta) &\leq 15D^{D^3-3} m^{20m8^g} H_1 \\ &\leq D^{D^3-1} (4D^2)^{20m8^g} H_1 \\ &\leq 2^{D(D^3-1)/2+(D+2)20m8^g} H_1 \\ &\leq 2^{D^4/2+20D^4 8^g} H_1 \end{aligned}$$

(où à chaque étape nous tirons profit des majorations faites dans la preuve de la proposition 10.1 de [R2]). Nous estimons encore $2^{164g} \leq 2^{82D^2} \leq 2^{6D^4}$ pour aboutir à

$$2^{164g} \max(1, h_\theta) \leq 2^{21D^4 8^g - 1} H_1.$$

Il reste à constater que $21D^4 8^g$ est au plus 3^{D^2} (avec $g \leq (D-1)(D-2)/2$).

Ensuite, dans la démonstration de la proposition 10.2, nous modifions simplement la dernière majoration pour écrire

$$D^{12}[K : \mathbb{Q}] \log(h_\infty(F) + 2) \leq 2D^{12}[K : \mathbb{Q}]^4 H_1$$

et retrouver la même borne que précédemment grâce à l'estimation très large $2D^{12} \leq 2^{3D^2}$.

Il n'y a rien à changer au lemme 10.1 qui utilise seulement que la borne doit être supérieure à D^2 . Pour montrer l'analogie du lemme 10.2, en suivant son argument (et ses notations), il nous suffit de montrer

$$\sum_{i=1}^s 2^{3D_i^2} (4D + 1) \leq 2^{3D^2}$$

ou encore

$$5D^2 2^{3(D-2)^2} \leq 2^{3D^2}.$$

Ceci est à nouveau très largement vérifié et permet donc de terminer la démonstration du théorème 2. Le théorème 1 s'en déduit immédiatement par $h_\infty(F) \leq \log M$ et $[K : \mathbb{Q}] = \Delta_{K/\mathbb{Q}} = 1$.

Bibliographie

- [DP] S. DAVID ET P. PHILIPPON, *Minors des hauteurs normalisées des sous-variétés de variétés abéliennes*. Comment. Math. Helv. **77** (2002), 639–700.
- [R1] G. RÉMOND, *Décompte dans une conjecture de Lang*. Invent. math. **142** (2000), 513–545.
- [R2] G. RÉMOND, *Nombre de points rationnels des courbes*. Proc. London Math. Soc. **101** (2010), 759–794.

Gaël RÉMOND
Institut Fourier, UMR 5582
BP 74
38402 Saint-Martin-d'Hères Cedex, France
E-mail: `Gael.Remond@ujf-grenoble.fr`