ACTA ARITHMETICA
174.2 (2016)

Contre-exemples au principe de Hasse pour les courbes de Fermat

par

Alain Kraus (Paris)

Introduction. Soit $p \geq 3$ un nombre premier. Une *courbe de Fermat* $C/\mathbb{Q}$ d'exposant p est définie par une équation de la forme

$$ax^p + by^p + cz^p = 0,$$

où a, b, c sont des entiers rationnels non nuls. On s'intéresse dans cet article au comportement de ces courbes vis-à-vis du principe de Hasse. Adoptons la terminologie en vigueur selon laquelle C présente une obstruction locale en un nombre premier ℓ si $C(\mathbb{Q}_\ell)$ est vide. On dit que la courbe C *contredit le principe de Hasse* si elle ne présente aucune obstruction locale et si $C(\mathbb{Q})$ est vide. La place à l'infini n'intervient pas ici car $C(\mathbb{R})$ est non vide.

Si a, b, c ne vérifient pas de relation linéaire non triviale à coefficients dans $\{-1, 0, 1\}$, il est très fréquent que C possède au moins une obstruction locale [H-K]. On se préoccupe ici du problème d'expliciter des courbes de Fermat contredisant le principe de Hasse. À ma connaissance, l'état de ce problème est le suivant. Historiquement, le premier exemple qui a été découvert à ce sujet est la courbe d'équation

$$3x^3 + 4y^3 + 5z^3 = 0,$$

explicitée par E. S. Selmer [Se] en 1951. Par ailleurs, il figure dans [H-K] des exemples de courbes de Fermat contredisant ce principe pour tout p au moins 5 plus petit que 100. Ils ont été obtenus par des techniques modulaires liées aux représentations galoisennes des points de torsion des courbes elliptiques. H. Cohen [Co, Cor. 6.4.11] a également obtenu de tels exemples pour $p \leq 11$ par une approche cyclotomique. Cela étant, on ne sait pas démontrer que pour tout p, il existe une courbe de Fermat d'exposant p contredisant le

2010 *Mathematics Subject Classification*: Primary 11D41.
Key words and phrases: Fermat curves, counterexample to the Hasse principle.
Received 23 January 2016; revised 13 April 2016.
Published online 13 June 2016.

DOI: 10.4064/aa8420-4-2016

principe de Hasse. Néanmoins, certains résultats établis dans [H-K] rendent plausible la conjecture suivante :

CONJECTURE. *Pour tout nombre premier $p \geq 3$, il existe une infinité de courbes de Fermat d'exposant p, deux à deux non $\mathbb{Q}$-isomorphes, contredisant le principe de Hasse.*

C'est une conséquence de la conjecture abc pour $p \geq 5$ (*loc. cit.*, prop. 5.1). Le nombre premier p étant donné, on obtient ici un critère impliquant cet énoncé pour l'exposant p. Cela permet d'en déduire cette conjecture pour $p \leq 19$. La méthode que l'on utilise repose sur l'approche cyclotomique présentée par H. Cohen [Co], ainsi que sur le théorème de densité de Chebotarev. Elle permet par ailleurs, pour $p \leq 19$, d'expliciter de nombreuses courbes de Fermat d'exposant p contredisant le principe de Hasse.

Tous les calculs numériques que ce travail a nécessités ont été effectués avec le logiciel de calcul Pari [Pa].

I. Énoncé des résultats. Soient $p \geq 3$ un nombre premier et $c \geq 2$ un entier sans puissances p-ièmes. Pour tout nombre premier ℓ, désignons par $C_\ell/\mathbb{Q}$ la courbe d'équation

$$x^p + \ell y^p + cz^p = 0.$$

Posons $K = \mathbb{Q}(\sqrt[p]{c})$ et notons :

- O_K son anneau d'entiers,
- f l'indice de $\mathbb{Z}[\sqrt[p]{c}]$ dans O_K,
- Cl_K le groupe des classes de K,
- h_K le nombre de classes de K.

On supposera dans toute la suite que p divise h_K. Notons par ailleurs :

- e l'exposant du groupe abélien Cl_K,
- r la valuation p-adique de e,
- N le nombre de copies de $\mathbb{Z}/p^r\mathbb{Z}$ intervenant dans la décomposition primaire de Cl_K,
- S l'ensemble des nombres premiers $\ell \not\equiv 1 \bmod p$, ne divisant pas f, tels que la courbe $C_\ell/\mathbb{Q}$ ne présente aucune obstruction locale.

Pour tout $\ell \in S$, il existe un unique idéal premier de O_K au-dessus de ℓ de degré résiduel 1 (lemme 1). Notons finalement

- S_0 le sous-ensemble de S formé des nombres premiers ℓ tels que la condition suivante soit satisfaite :
  si $\mathfrak{q}$ est l'idéal premier de O_K au-dessus de ℓ de degré résiduel 1, l'idéal $\mathfrak{q}^{e/p}$ n'est pas principal.

THÉORÈME. *Supposons que les deux conditions suivantes soient remplies :*

(1) $c^{p-1} \not\equiv 1 \bmod p^2$.
(2) p *divise* h_K.

Alors, pour tout $\ell \in S_0$ *la courbe* $C_\ell/\mathbb{Q}$ *est un contre-exemple au principe de Hasse. Si* S *a une densité strictement plus grande que* $1/p^N$*, l'ensemble* S_0 *est infini, auquel cas la conjecture est vraie pour l'exposant* p.

COROLLAIRE. *Supposons que* (p, c) *soit l'un des couples suivants :*

$$(3, 921),\ (5, 19),\ (7, 13),\ (11, 373),\ (13, 103),\ (17, 1087),\ (19, 37).$$

Alors S_0 *est infini. En particulier, la conjecture est vraie pour* $p \leq 19$.

REMARQUE 1. L'énoncé du théorème permet d'obtenir de nombreux contre-exemples au principe de Hasse. À titre indicatif, pour $(p, c) = (5, 19)$, on a $h_K = 5$ et il y a 72 classes de nombres premiers ℓ modulo 275 qui sont dans S. Pour chaque nombre premier ℓ dans l'une de ces classes, si ℓ est dans S_0, alors C_ℓ est un contre-exemple au principe de Hasse. Par exemple, l'ensemble des nombres premiers congrus à 7 modulo 275 est l'une de ces classes. Il y a 48 nombres premiers plus petits que 10^5 congrus à 7 modulo 275, et il y en a 31 qui sont dans S_0. Le plus petit d'entre eux est 1657 et le plus grand est 95707.

REMARQUE 2. Si l'on essaye d'étendre l'énoncé du corollaire avec des nombres premiers $p \geq 23$, cela devient, a priori, nettement plus couteux numériquement. Par exemple, afin de pouvoir conclure pour $p = 23$, il semble qu'il faille disposer de valeurs de c pour lesquelles Cl_K contienne un sous-groupe isomorphe à $\mathbb{Z}/23\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$.

II. Démonstration du théorème. Commençons par établir trois lemmes préliminaires.

LEMME 1. *Soit* ℓ *un nombre premier ne divisant pas* f *tel que l'on ait* $\ell \not\equiv 1 \bmod p$. *Il existe un unique idéal premier de* O_K *au-dessus de* ℓ *de degré résiduel* 1.

Démonstration. Posons $F = X^p - c$. La condition $\ell \not\equiv 1 \bmod p$ entraîne que 1 est la seule racine p-ième de l'unité dans $\mathbb{F}_\ell$, donc le morphisme $\mathbb{F}_\ell^* \to \mathbb{F}_\ell^*$ qui à x associe x^p est bijectif. Par suite, F a une unique racine dans $\mathbb{F}_\ell$. Parce que ℓ ne divise pas f, cela entraîne le résultat.

LEMME 2. *Soit* ℓ *un nombre premier ne divisant pas* cf *tel que l'on ait* $\ell \equiv 1 \bmod p$. *Alors,* ℓ *est inerte ou totalement décomposé dans* K.

Démonstration. Les racines p-ièmes de l'unité sont dans $\mathbb{F}_\ell$ car p divise $\ell - 1$. Si le polynôme $F = X^p - c$ n'a pas de racines dans $\mathbb{F}_\ell$, alors F est

irréductible modulo ℓ et ℓ est donc inerte dans K. Sinon, F a toutes ses racines dans $\mathbb{F}_\ell$, donc possède p racines distinctes dans $\mathbb{F}_\ell$ (ℓ ne divise pas c), et ℓ est totalement décomposé dans K.

Lemme 3. *La densité des nombres premiers totalement décomposés dans K est $1/(p(p-1))$.*

Démonstration. Un nombre premier est totalement décomposé dans K si et seulement si il est totalement décomposé dans la clôture galoisienne de K, qui est de degré $p(p-1)$ sur $\mathbb{Q}$, d'où l'assertion.

Considérons alors un nombre premier $\ell \in S_0$. Vérifions que $C_\ell(\mathbb{Q})$ est vide, ce qui établira que $C_\ell/\mathbb{Q}$ est un contre-exemple au principe de Hasse.

On utilise pour cela [Co, théorème 6.4.8]. Rappelons par commodité son énoncé adapté à notre objectif. Suivant la terminologie utilisée dans *loc. cit.*, en tenant compte du fait que ℓ ne divise pas f, on dit qu'un idéal $\mathfrak{b}$ de O_K divisant ℓO_K est un *diviseur convenable* de ℓ si les trois conditions suivantes sont remplies :

- $\mathfrak{b}$ et $\ell O_K/\mathfrak{b}$ sont primitifs (un idéal $\mathfrak{a}$ de O_K est dit *primitif* si $m = 1$ est le seul entier naturel m tel que $\mathfrak{a}/m$ soit un idéal entier).
- $\ell/\mathrm{N}\,\mathfrak{b}$ est la puissance p-ième d'un nombre rationnel, où $\mathrm{N}\,\mathfrak{b}$ est la norme de K sur $\mathbb{Q}$ de $\mathfrak{b}$.
- Tous les idéaux premiers de O_K divisant $\mathfrak{b}$ sont de degré résiduel 1.

Théorème (Cohen). *Supposons que les conditions suivantes soient satisfaites :*

(1) $c^{p-1} \not\equiv 1 \bmod p^2$.
(2) *p divise h_K.*
(3) *Pour chaque diviseur convenable $\mathfrak{b}$ de ℓ, l'idéal $\mathfrak{b}^{e/p}$ n'est pas principal.*

Alors, $C_\ell(\mathbb{Q})$ est vide.

Les deux premières conditions sont par hypothèse satisfaites. Le seul diviseur convenable de ℓ est l'idéal premier $\mathfrak{q}$ de O_K au-dessus de ℓ de degré résiduel 1 (lemme 1). Le nombre premier ℓ étant dans S_0, l'idéal $\mathfrak{q}^{e/p}$ n'est pas principal, donc la troisième condition est aussi satisfaite. Le théorème de Cohen entraîne alors que $C_\ell(\mathbb{Q})$ est vide.

Supposons S de densité strictement plus grande que $1/p^N$. Démontrons que S_0 est infini et par suite que la conjecture est vraie pour l'exposant p.

Proposition 1. *Soit A un ensemble de nombres premiers non congrus à 1 modulo p. Soit B l'ensemble des idéaux premiers de O_K de degré résiduel 1 au-dessus d'un nombre premier de A. Alors, si A a une densité, il en est de même de B et elles sont égales.*

Démonstration. Pour tout idéal premier $\mathfrak{p}$ de O_K, notons $\mathrm{N}\,\mathfrak{p}$ sa norme sur $\mathbb{Q}$ et $\deg\mathfrak{p}$ son degré résiduel. Si $\mathfrak{p}$ est au-dessus du nombre premier ℓ, on a $\mathrm{N}\,\mathfrak{p} = \ell^{\deg\mathfrak{p}}$. Supposons A de densité d. Pour tout $x > 0$ posons

$$u(x) = \frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x\}|}.$$

Il s'agit d'établir que $u(x)$ a une limite égale à d quand x tend vers l'infini. On a

$$u(x) = \frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}|} \cdot \frac{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}|}{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x\}|}.$$

D'après les lemmes 1 et 2, il existe une constante c_1 telle que

$$|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}| = |\{\ell \mid \ell \le x,\ \ell \not\equiv 1 \bmod p\}| + p \cdot |\{\ell \mid \ell \le x,\ \ell \text{ totalement décomposé dans } K\}| + c_1.$$

Notons $\pi(x)$ le nombre des nombres premiers plus petits que x et posons

$$v(x) = \frac{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}|}{\pi(x)}.$$

D'après le théorème de Dirichlet et le lemme 3, la fonction $v(x)$ a une limite quand x tend vers l'infini, qui vaut ainsi

$$\frac{p-2}{p-1} + p \cdot \frac{1}{p(p-1)} = 1.$$

On écrit alors

$$\frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}|} = \frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{\pi(x)} \cdot \frac{1}{v(x)}.$$

Les nombres premiers de A étant non congrus à 1 modulo p, il existe une constante c_2 telle que l'on ait (lemme 1)

$$|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}| = |\{\ell \mid \ell \le x,\ \ell \in S\}| + c_2.$$

Puisque A est de densité d, on obtient

$$\lim_{x\to\infty} \frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{\pi(x)} = d.$$

Par suite,

$$\lim_{x\to\infty} \frac{|\{\mathfrak{p} \in B \mid \mathrm{N}\,\mathfrak{p} \le x\}|}{|\{\mathfrak{p} \mid \mathrm{N}\,\mathfrak{p} \le x,\ \deg\mathfrak{p} = 1\}|} = d.$$

L'ensemble des idéaux premiers de O_K de degré 1 étant de densité 1, la limite de $u(x)$ vaut donc d, d'où le résultat.

Remarque 3. L'énoncé de la proposition 1 est faux si on enlève l'hypothèse « non congrus à 1 modulo p », comme on le constate en prenant pour A l'ensemble des nombres premiers inertes dans K. En effet, d'après les lemmes 1 et 2 ainsi que le théorème de Dirichlet, la densité des nombres premiers

totalement décomposés dans K ou inertes dans K est $1/(p-1)$. La densité des nombres premiers inertes est donc $1/(p-1) - 1/(p(p-1)) = 1/p$.

PROPOSITION 2. *Soit S_1 l'ensemble des idéaux premiers $\mathfrak{q}$ de O_K tels que $\mathfrak{q}^{e/p}$ soit principal. Alors, S_1 a une densité égale à $1/p^N$.*

Démonstration. Un idéal premier $\mathfrak{q}$ de O_K appartient à S_1 si et seulement si l'ordre de la classe de $\mathfrak{q}$ dans Cl_K n'est pas divisible par p^r. Le nombre d'éléments de $\mathbb{Z}/p^r\mathbb{Z}$ qui ne sont pas d'ordre p^r est p^{r-1}. Ainsi, dans un produit de N copies de $\mathbb{Z}/p^r\mathbb{Z}$, il y a $p^{N(r-1)}$ éléments dont l'ordre n'est pas divisible par p^r. Le nombre d'éléments de Cl_K d'ordre non divisible par p^r est donc

$$p^{N(r-1)}\frac{h_K}{p^{rN}} = \frac{h_K}{p^N}.$$

Par ailleurs, il y a une densité de $1/h_K$ d'idéaux premiers de O_K dans chaque classe d'idéaux de K, d'où le résultat.

Fin de la démonstration du théorème. D'après la proposition 1, utilisée avec $A = S$, et l'hypothèse faite sur S, l'ensemble T des idéaux premiers de O_K de degré 1 au-dessus d'un nombre premier de S est de densité strictement plus grande que $1/p^N$. D'après la proposition 2, il existe donc une infinité d'idéaux premiers $\mathfrak{q}$ de T tels que $\mathfrak{q}^{e/p}$ ne soit pas principal. Cela entraîne que S_0 est infini.

Il reste à remarquer que si ℓ et ℓ' sont deux nombres premiers distincts, ne divisant pas c, la jacobienne de C_ℓ a bonne réduction en ℓ' mais pas en ℓ, et de même pour $C_{\ell'}$. En particulier, les courbes C_ℓ et $C_{\ell'}$ ne sont pas $\mathbb{Q}$-isomorphes, d'où le théorème.

III. Démonstration du corollaire. Soit p un nombre premier fixé. Suivant la terminologie adoptée dans [H-K, §3], on dira qu'un nombre premier q est *exceptionnel pour p* si $q \neq p$ et s'il existe a, b, c non nuls dans $\mathbb{F}_q$ tels que la courbe de Fermat d'équation $ax^p + by^p + cz^p = 0$ ne possède pas de points rationnels sur $\mathbb{F}_q$. D'après les travaux de Weil, les nombres premiers exceptionnels pour p sont plus petits que $((p-1)(p-2))^2$ ([We]). En particulier, ils sont explicitables. Par ailleurs, ils sont congrus à 1 modulo p. Afin d'établir qu'une courbe C_ℓ n'a pas d'obstructions locales, il suffit de vérifier que pour tout nombre premier q divisant $p\ell c$ ou qui est exceptionnel pour p, l'ensemble $C_\ell(\mathbb{Q}_q)$ est non vide. Dans le cas où ℓ, p, c sont premiers entre eux deux à deux, on a utilisé pour cela les quatre assertions suivantes que l'on rappelle ici par commodité [H-K, Lemme 3.1]:

- Pour que $C_\ell(\mathbb{Q}_p)$ soit non vide il faut et il suffit qu'il existe des entiers rationnels x, y, z, pas tous multiples de p, tels que
$$x^p + \ell y^p + cz^p \equiv 0 \bmod p^2.$$

- Soit q un nombre premier ne divisant pas $p\ell c$. Pour que $\mathbb{C}_\ell(\mathbb{Q}_q)$ soit non vide il faut et il suffit que $C_\ell(\mathbb{F}_q)$ soit non vide.
- Pour que $C_\ell(\mathbb{Q}_\ell)$ soit non vide il faut et il suffit que la classe de c soit une puissance p-ième dans $\mathbb{F}_\ell$.
- Soit q un nombre premier divisant c. Pour que $C_\ell(\mathbb{Q}_q)$ soit non vide il faut et il suffit que la classe de ℓ soit une puissance p-ième dans $\mathbb{F}_q$. Tel est le cas si $q \not\equiv 1 \bmod p$.

Pour chaque couple (p, c), notons d la densité de l'ensemble S correspondant.

Supposons $(p, c) = (3, 921)$. On a $c^2 \not\equiv 1 \bmod 9$ et le groupe des classes du corps $K = \mathbb{Q}\big(\sqrt[3]{921}\big)$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Ainsi $N = 2$. Il n'y a pas de nombres premiers exceptionnels pour $p = 3$. Par suite, C_ℓ n'a pas d'obstructions locales si et seulement si $C_\ell(\mathbb{Q}_3)$, $C_\ell(\mathbb{Q}_\ell)$ et $C_\ell(\mathbb{Q}_{307})$ sont non vides.

Soit ℓ un nombre premier congru à 2 modulo 3. On est dans le cas où p divise c. En utilisant le lemme de Hensel, on vérifie alors que $C_\ell(\mathbb{Q}_3)$ est non vide. De même, $C_\ell(\mathbb{Q}_\ell)$ est non vide, car tout élément de $\mathbb{F}_\ell$ est un cube dans $\mathbb{F}_\ell$. Par ailleurs, on trouve 102 classes de nombres premiers ℓ modulo 307 pour lesquelles $C_\ell(\mathbb{Q}_{307})$ est non vide. On obtient ainsi 102 classes de nombres premiers ℓ modulo 921 pour lesquelles C_ℓ n'a pas d'obstructions locales. En notant φ la fonction indicatrice d'Euler, on en déduit que

$$d = \frac{102}{\varphi(921)} = \frac{1}{6}.$$

On a $d > 1/9$, d'où le résultat dans ce cas.

Supposons $(p, c) = (5, 19)$. On a $c^4 \not\equiv 1 \bmod 25$ et $h_K = 5$, en particulier $N = 1$. Soit ℓ un nombre premier non congru à 1 modulo 5 et distinct de 5. Parce que 11 est le seul nombre premier exceptionnel pour $p = 5$, la courbe C_ℓ n'a pas d'obstructions locales si et seulement si

$$C_\ell(\mathbb{Q}_5),\ C_\ell(\mathbb{Q}_\ell),\ C_\ell(\mathbb{Q}_{19}),\ C_\ell(\mathbb{Q}_{11})$$

ne sont pas vides. Tel est le cas de $C_\ell(\mathbb{Q}_\ell)$ et de $C_\ell(\mathbb{Q}_{19})$ car tout élément de $\mathbb{F}_\ell$ et de $\mathbb{F}_{19}$ est une puissance 5-ième. On constate que $C_\ell(\mathbb{Q}_5)$ est non vide si et seulement si

$$\ell \equiv 7, 8, 9, 12, 13, 17, 18, 19, 24 \bmod 25.$$

Par ailleurs, $C_\ell(\mathbb{Q}_{11})$ est non vide si et seulement si

$$\ell \equiv 1, 2, 3, 4, 7, 8, 9, 10 \bmod 11.$$

On obtient ainsi 72 classes de nombres premiers ℓ modulo 275 pour lesquelles $C_\ell/\mathbb{Q}$ n'a pas d'obstructions locales. Il en résulte que

$$d = \frac{9}{25}.$$

On a $d > 1/5$, d'où le résultat.

Pour chaque couple (p, c) considéré ci-dessous, on présente les résultats numériques dans des tableaux à deux entrées q et N_q, qui se lisent de la façon suivante. L'entier q parcourt la réunion de $\{p\}$ et de l'ensemble des nombres premiers exceptionnels pour p. L'entier N_p est le nombre de classes de nombres premiers ℓ modulo p^2, avec $\ell \not\equiv 1 \bmod p$, pour lesquelles $C_\ell(\mathbb{Q}_p)$ est non vide. Si $q \neq p$, N_q est le nombre de classes de nombres premiers ℓ modulo q pour lesquelles $C_\ell(\mathbb{Q}_q)$ est non vide.

Par ailleurs, c est premier, on a $c \not\equiv 1 \bmod p$ et $c^{p-1} \not\equiv 1 \bmod p^2$. Pour tout nombre premier $\ell \not\equiv 1 \bmod p$ et distinct de p, $C_\ell(\mathbb{Q}_\ell)$ est non vide. De même, $C_\ell(\mathbb{Q}_c)$ est non vide.

On obtient les résultats suivants.

Pour $(p, c) = (7, 13)$, on a $h_K = 7$,

q	7	29	43	71
N_q	25	16	30	60

d'où

$$d = \frac{25 \times 16 \times 30 \times 60}{\varphi(49 \times 29 \times 43 \times 71)} = \frac{500}{2401} > \frac{1}{7}.$$

Pour $(p, c) = (11, 373)$, Cl_K est isomorphe à $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. On obtient

q	11	23	67	89	199	419
N_q	54	8	66	56	162	380

d'où

$$d = \frac{13608}{161051} > \frac{1}{121}.$$

Pour $(p, c) = (13, 103)$, on a $h_K = 13$,

q	13	53	79	131	157	313	547
N_q	99	24	78	80	108	240	546

d'où

$$d = \frac{35640}{371293} > \frac{1}{13}.$$

Pour $(p, c) = (17, 1087)$, on a $h_K = 17$,

q	17	103	137	239	307	409	443	613	647	919	953	1021	1123	1429
N_q	165	102	56	168	252	360	416	612	608	918	952	1020	1056	1428

d'où

$$d = \frac{745113600}{6975757441} > \frac{1}{17}.$$

Pour $(p,c)=(19,37)$, on a $h_K=19$,

q	19	191	229	419	457	571	647	761	1103	1597
N_q	187	100	144	374	312	450	646	720	986	1512

d'où

$$d=\frac{22762911600}{322687697779}>\frac{1}{19}.$$

Cela termine la démonstration du corollaire.

Remerciements. Je remercie D. Bernardi pour ses remarques concernant cet article, ainsi que le referee pour les commentaires dont il m'a fait part.

Références

[Co] H. Cohen, *Number Theory. Vol. I: Tools and Diophantine Equations*, Grad. Texts in Math. 239, Springer, 2007.

[H-K] E. Halberstadt et A. Kraus, *Courbes de Fermat : résultats et problèmes*, J. Reine Angew. Math. 548 (2002), 167–234.

[Pa] C. Batut, D. Bernardi, K. Belabas, H. Cohen et M. Olivier, *PARI-GP, version 2.7.3*, Univ. de Bordeaux I, 2015.

[Se] E. S. Selmer, *The Diophantine equation* $ax^3+by^3+cz^3=0$, Acta Math. 85 (1951), 203–362.

[We] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, 1948.

Alain Kraus
Université de Paris VI
Institut de Mathématiques de Jussieu
4 Place Jussieu
75005 Paris, France
E-mail: alain.kraus@imj-prg.fr