TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 343, Number 2, June 1994

LE THÉORÈME DE FERMAT-GOSS

LAURENT DENIS

ABSTRACT. The analogue of the Fermat equation and of the Fermat conjecture is studied by Goss [G], on the rational function fields in characteristic $p > 0$. We prove here that this equation has no nontrivial solutions. When $q = 2$, the method uses the canonical height on the t-module constructed in [D]. This method also gives finiteness theorems for some generalization of the Fermat equation in higher dimension.

1. POSITION DU PROBLÈME

On désigne par $A = \mathbf{F}_q[T]$, l'anneau des polynômes en une variable sur le corps fini à q éléments $\mathbf{F}_q$ de caractéristique p, par $k = \mathbf{F}_q(T)$ son corps des fractions, par $k_\infty = \mathbf{F}_q((1/T))$ son complété pour la valuation $1/T$-adique, $\overline{k_\infty}$ une clôture algébrique de k_∞ et par $\overline{k}$ la clôture algébrique de k dans $\overline{k_\infty}$. On note $\deg(a)$ le degré d'un élément a de A avec la convention $\deg(0) = -\infty$.

Le module de Carlitz est alors la donnée $(\mathbf{G_a}, \Phi)$ du groupe additif $\mathbf{G_a}$ et d'un homomorphisme d'anneau injectif: $\Phi\colon \mathbf{F}_q[T] \hookrightarrow \mathrm{End}_{\overline{k_\infty}}(\mathbf{G_a})$ déterminé par $\Phi(T) = TF^0 + F$, où F est le Frobenius relatif à $\mathbf{F}_q$.

D. Goss, a montré dans [G] qu'un bon analogue homogène de l'équation de Fermat est

$$[a, q]_1 \qquad Y^{q^r}(\Phi(a)(X/Y)) = Z^{q^r}$$

et qu'un bon analogue non homogène est:

$$[a, q]_2 \qquad Y^{q^r}(\Phi(a)(X/Y)) = Z^{p}$$

où a est fixé unitaire dans A de degré $r \geq 1$. Goss a entre autre prouvé que si a est irréductible et régulier (cf. [G]), de degré > 1 alors pour $q \neq 2$, $[a, q]_2$ et donc $[a, q]_1$ n'a pas de solution avec X, Y, $Z \in A$ et $XYZ \neq 0$. Puis il a montré que si $[ab, q]_1$ (resp. $[ab, q]_2$) possède une solution avec $XYZ \neq 0$, alors il en est de même pour $[a, q]_1$ et $[b, q]_1$ (resp. pour $[a, q]_2$ et $[b, q]_2$).

Ces propriétés sont analogues à celles de l'équation $X^n - Y^n = Z^n$. La construction initiale de cette analogie repose sur la remarque qu'une éventuelle solution satisfait

$$Y^n((X/Y)^n - 1) = Z^n;$$

Les racines de $w^n - 1 = 0$, sont les racines de l'unité dont l'analogie avec les points de torsion (i.e., les racines de $\Phi(a)X = 0$), a conduit D. Hayes à

Received by the editors July 8, 1992 and, in revised form, October 19, 1992.
1991 *Mathematics Subject Classification*. Primary 11G09; Secondary 11J25.

l'analogue de la théorie cyclotomique (cf. [H]). Notons enfin que l'exposant n du problème de Fermat classique peut être vu comme une valeur absolue, ce qui justifie les puissances q-ièmes dans l'équation homogène.

Les solutions avec $XYZ = 0$ sont dites triviales. Remarquons que si on a une solution (X, Y, Z) non triviale d'une de ces équations, alors on en a une avec $(X, Y) = 1$ et $(Z, Y) = 1$. Dans toute la suite toutes les solutions considérées sont de ce type. On prouve

Proposition 1. *Si* $q \neq 2$ *et* $\deg(a) > 1$, *ou si* $q = 2$ *et* $\deg(a) > 2$, $[a, q]_1$ *et* $[a, q]_2$ *n'ont qu'un nombre fini de solutions* (X, Y, Z) *avec* $(X, Y) = 1$ *et* $(Z, Y) = 1$.

Remarque 1. Si $\deg(a) = 1$, Goss a montré qu'il peut y avoir une infinité de solutions, poursuivant en cela l'analogie avec $X^2 - Y^2 = Z^2$.

Remarque 2. Le résultat est effectif, on peut majorer la hauteur des solutions en fonction de q et de $\deg(a)$.

Remarque 3. La version qualitative de cette proposition pour $[a, q]_1$ découle également des analogues de la conjecture de Mordell démontrées par Samuel (cf. [S], voir aussi le papier de Voloch [V]).

Les résultats principaux sont démontrés aux §§3 et 4. On prouve qu'hormis les cas décrit par Goss dans [G], les équations de Fermat n'ont aucune solution non triviale.

Théorème 1. *Si* $q \geq 3$ *et* $\deg(a) \geq 2$, $[a, q]_1$ *n'a aucune solution non triviale.*

Pour $[a, q]_2$, on prouve

Théorème 2. *Si* $q \geq 3$, $p \neq 2$, $\deg(a) \geq 2$, *alors* $[a, q]_2$ *n'a aucune solution non triviale.*

Théorème 3. *Si* $q \geq 4$, $p = 2$, $\deg(a) \geq 2$, *alors* $[a, q]_2$ *a une solution uniquement dans le cas où* $a = (T^2 + T + \beta)$, *où* β *est un carré de* $\mathbf{F}_q$ *et cette solution est alors proportionnelle dans* $\mathbf{F}_q$ *au triplet* $(1, 1, T + T^{q/2})$.

Enfin, dans le cas $q = 2$

Théorème 4. *Si* $q = 2$, $\deg(a) \geq 4$, *alors* $[a, q]_1$ *et* $[a, q]_2$ *a une solution uniquement dans le cas où a est de la forme* $(T^2 + T)b(T) + 1$ *et cette solution est* $(1, 1, 1)$.

Remarque 4. Les cas $\deg(a) = 2$ et $\deg(a) = 3$ sont également traités au §4.

Remarque 5. Grâce à la $\mathbf{F}_q$ linéarité de Φ, on peut également obtenir les résultats sans supposer a unitaire.

Après quelques préliminaires au §2, les démonstrations des Théorèmes 1, 2, 3 sont données au §3. Le Théorème 4 est démontré au §4. Le dernier paragraphe donne des énoncés de finitude pour des systèmes d'équations qui apparaissent naturellement quand on considère des t-modules plus généraux (cf. [A]) que le module de Carlitz. Dans le cas des modules de Drinfeld (voir §5), on obtient

Proposition 2. *Soit* $\Phi(t) = a_0F^0 + \cdots + a_dF^d$ *un t-module de dimension* 1 *défini sur* $\mathbf{F}_q(T)$ *et* h *le plus grand indice tel que* $a_h' \neq 0$. *On suppose* $h \geq 1$,

$q^h - 2 > 0$, *alors l'équation* (Φ, q) *a au plus un nombre fini de solutions non triviales avec* $(X, Y) = 1$.

L'auteur remercie D. Goss et D. Thakur pour leurs utiles suggestions qui m'ont permis d'améliorer de nombreux passages de ce texte.

2. Lemmes préliminaires

On prouve plusieurs lemmes concernant le degré des coefficients du module de Carlitz et celui de leur dérivée.

Lemme 1. *Soit* $r = \deg(a) \geq 1$ *et* $(a_1, \ldots, a_r)$ *définis par*

$$\Phi(a) = aF^0 + a_1F + \cdots + a_rF^r;$$

alors $a'_{r-1} \in (\mathbf{F}_q)^*$ *(où* $'$ *désigne la dérivation par rapport à* T*), et si* a *est unitaire* $a'_{r-1} = 1$.

Preuve. Il suffit de le montrer quand a est une puissance de T. On remarque que $\Phi(T^i)$ a 1 comme coefficient de F^i. On écrit $\Phi(T^i) = T^iF^0 + a_1F + \cdots + a_{i-1}F^{i-1} + F^i$. Comme $\Phi(T^i) = \Phi(T)\Phi(T^{i-1})$, et que $\Phi(T) = TF^0 + F$, a_{i-1} est égal à la somme de T et de puissances q-ièmes.

Lemme 2. *Soit a dans* A *de degré* $r \geq 1$, *on écrit* $\Phi(a) = aF^0 + a_1F + \cdots + a_rF^r$; *alors:* $\deg(a_i) = q^i \deg(a) - iq^i$, $\deg(a'_i) \leq q^i(\deg(a) - i) - 1$ *et* $\deg(a'_{r-1}) = 0$.

Preuve. Comme $\Phi(a)$ et $\Phi(T)$ commutent on a

$$a_i = \frac{a_{i-1}^q - a_{i-1}}{T^{q^i} - T}.$$

On déduit aisément: $\deg(a_i) = q^i \deg(a) - iq^i$ $(0 \leq i \leq \deg(a))$. D'où $\deg(a'_i) \leq q^i \deg(a) - iq^i - 1$ $(\deg(a'_{r-1}) = 0$ a été vu au Lemme 1).

Lemme 3. *Soit a de degré* $r \geq 3$ *(ou* $r = 2$ *et* $p \neq 2$*) et* $\Phi(a) = aF^0 + a_1F + \cdots + a_rF^r$. *Le coefficient* a_{r-2} *n'est pas une puissance p-ième. De plus ce coefficient contient la puissance strictement maximale de* T *qui n'est pas une puissance p-ième parmi les coefficients* a_i $(0 \leq i \leq r)$.

Preuve. On voit facilement par récurrence sur le degré $s \geq 1$ d'un élément b de A, que le terme de plus haut degré en T de $\Phi(b)$ est $T^{q^{s-1}}$. Pour $r = \deg(a) \geq 2$, la division euclidienne par T s'écrit $a = Tb + c$. Il suit, $\Phi(a) = \Phi(T)(\Phi(b)) + c$. Comme le terme de plus haut degré en T de $\Phi(b)$ est $T^{q^{r-2}}$, a_{r-2} contient un terme en $T^{(q^{r-2}+1)}$ et les termes de degré supérieur qui apparaissent dans les a_i sont des puissances p-ièmes. Le lemme découle alors clairement de cette propriété car $r \geq 3$ ou $r = 2$ et $p \neq 2$.

Ces trois lemmes suffisent pour étudier le cas $q \neq 2$. Donnons maintenant des résultats sur les hauteurs, qui permettront de traiter le cas $q = 2$, mais que l'on énonce pour q quelconque.

Rappelons que si x, $y \in A$ sont premiers entre eux la hauteur de Weil de x/y est définie par $h(x/y) = \max(\deg(x), \deg(y))$.

Lemme 4. *Soient* $(b_0, \ldots, b_r)$ *des éléments de* k. *On pose* $\Psi(T) = b_0F^0 + b_1F + \cdots + b_rF^r$. *Dès que* $r \geq 1$ *et* $b_r \neq 0$ *on a les propriétés suivantes:*

(a) *Il existe une unique fonction* $\hat{h}_\Psi : \mathbf{G_a}(k) \to \mathbb{R}$, *vérifiant pour tout* $a \in A$ *et tout* $\alpha \in k$ *on* a

$$\hat{h}_\Psi(\Psi(a)(\alpha)) = q^{r\ \deg(a)}\hat{h}_\Psi(\alpha).$$

(b) *Il existe un réel* $C_\Psi > 0$, *ne dépendant que des coefficients* $(b_0, \dots, b_r)$ *et de* q *tel que si* h *désigne la hauteur de Weil usuelle on ait: pour tout* $\alpha \in k$, $|\hat{h}_\Psi(\alpha) - h(\alpha)| \leq C_\Psi$.

(c) $\hat{h}_\Psi(x) = \lim_{n\to\infty} q^{-nr}h(\Psi(T^n)(x))$.

Preuve. Comme $b_r \neq 0$, Ψ définit un module de Drinfeld de rang $r \geq 1$ et $\hat{h}_\Psi$ est alors la hauteur canonique associée à ce module (cf. [D, Théorème 1]).

Lemme 5. *Soit* $\Psi(T) = (1/a)[a_0F^0 + a_1F + \cdots + a_dF^d]$ *avec*

(i) $a, a_0, \dots, a_d \in A$,

(ii) $a_d \in A^*$,

(iii) $\deg(a_i) + q^i < q^d$, $0 \leq i \leq d-1$.

Désignons par $\hat{h}_\Psi$ *la hauteur canonique associée* (*cf.* *Lemme* 4). *Pour tout* $x \in k$, *on a*:

$$|\hat{h}_\Psi(x) - h(x)| \leq \frac{\max_{0\leq i\leq d-1}(\deg(a_i), \deg(a))}{q^d - 1}.$$

Preuve. On va estimer $h(\Psi(T)x)$ en fonction de $h(x)$. Soient P et Q deux éléments de A premiers entre eux. D'après le Lemme 1, on a l'expression suivante:

$$\Psi(T)\left(\frac{P}{Q}\right) = \frac{a_0PQ^{q^d-1} + a_1P^qQ^{q^d-q} + \cdots + a_dP^{q^d}}{aQ^{q^d}}.$$

Soit l un facteur premier de Q ne divisant pas a. Comme $a_d \in (\mathbf{F}_q)^*$, et que Q est premier à P, l ne divise pas le numérateur de l'expression précédente. On tire de là

(1)

$$\begin{aligned} q^d \deg(Q) &\leq h(\Psi(T)(P/Q)) \\ &\leq \max(\deg(a) + q^d\deg(Q), \max_{0\leq i\leq d}(\deg(a_i) + (q^d - q^i)\deg(Q) + q^i\deg(P))). \end{aligned}$$

Si $\deg(Q) \geq \deg(P)$, ceci s'écrit encore:

$$\begin{aligned} q^d\deg(Q) &\leq h(\Psi(T)(P/Q)) \\ &\leq \max(\deg(a) + q^d\deg(Q), \max_{0\leq i\leq d-1}(\deg(a_i) + q^d\deg(Q))); \end{aligned}$$

d'où:

$$0 \leq \frac{h(\Psi(T)(P/Q))}{q^d} - h\left(\frac{P}{Q}\right) \leq \frac{\max_{0\leq i\leq d-1}(\deg(a_i), \deg(a))}{q^d}.$$

Si $\deg(Q) < \deg(P)$, on utilise l'estimation $h(\Psi(T)(P/Q)) \geq M - \deg(a)$, où M est le degré du numérateur de $\Psi(T)(P/Q)$. Montrons que $M = q^d\deg(P)$. Il suffit de vérifier que

$$q^d\deg(P) > \max_{0\leq i\leq d-1}(\deg(a_i) + (q^d - q^i)\deg(Q) + q^i\deg(P)).$$

Comme $\deg(Q) \leq \deg(P) - 1$, il suffit d'avoir

$$q^d\deg(P) > \max_{0\leq i\leq d-1}(\deg(a_i) + (q^d - q^i)(\deg(P) - 1) + q^i\deg(P)),$$

ou encore

$$q^d > \max_{0\leq i\leq d-1} (\deg(a_i) + q^i),$$

c'est l'hypothèse (iii).

On obtient alors

$$-\deg(a) \leq h(\Psi(T)(P/Q)) - q^d h(P/Q).$$

Pour la majoration, on procède comme dans le cas $\deg(Q) \geq \deg(P)$ et on aboutit à la même majoration.

Dans tous les cas considérés on a donc montré

$$\left| \frac{h(\Psi(T)(P/Q))}{q^d} - h\left(\frac{P}{Q}\right) \right| \leq \frac{\max_{0\leq i\leq d-1}(\deg(a_i), \deg(a))}{q^d}.$$

Il suffit ensuite de se rappeller que $\hat{h}_\Psi(x) = \lim_n q^{-nd} h(\Psi(T^n)(x))$ et de sommer sur n pour avoir le Lemme 5.

Corollaire 1. *Etant donné a dans A de degré $r \geq 1$ et $\Phi(a) = aF^0 + a_1F + \cdots + a_rF^r$. Alors, $\Psi(T) = (1/a)[a'F^0 + a_1'F + \cdots + a_{r-1}'F^{r-1}]$, définit un module de Drinfeld de rang $r-1$ et la hauteur canonique associée $\hat{h}_\Psi$ vérifie la propriété suivante: si $r \geq 2$, pour tout $x \in k$:*

$$|\hat{h}_\Psi(x) - h(x)| \leq 2q^{r-2}/(q^{r-1} - 1).$$

Preuve. D'après le Lemme 1, Ψ définit un module de Drinfeld de rang $r-1$. On utilise alors les estimations données au Lemme 2, et on applique le résultat du Lemme 5.

Lemme 6. *Soit $\Phi(T) = TF^0 + F$, le module de Carlitz et $\hat{h}_\Phi$ la hauteur canonique associée. Pour tout $x \in k$, on a:*

$$\text{si } q \neq 2, \qquad |\hat{h}_\Phi(x) - h(x)| \leq 1/q,$$
$$\text{si } q = 2, \qquad |\hat{h}_\Phi(x) - h(x)| \leq 1.$$

Preuve. On écrit $x = P/Q$ avec P et Q premiers entre eux. On examine la hauteur de $\Phi(T)(P/Q)$, en faisant spécialement attention au cas $\deg(P) = \deg(Q)$ quand $q \neq 2$. Quand $q = 2$, le résultat est celui du Lemme 5 et est optimal si on prend $x = T$. On conclut de manière similaire au Lemme 5 (on peut en fait démontrer que $\hat{h}_\Phi(k) = \mathbb{N} \cup (\mathbb{N} + 1/q))$.

Rappelons enfin un lemme de Goss [G].

Lemme 7. *Soit (X, Y, Z) une solution de $[a, q]_1$ (resp. de $[a, q]_2$) avec $XYZ \neq 0$. Alors si $a = bc$ et $r' = \deg(c) \neq 0$. Le triplet $(U, V, W) = (\Phi(c)(X/Y)Y^{q^{r'}}, Y^{q^{r'}}, Z)$ (resp. $(\Phi(c)(X/Y)Y^{q^{r'}}, Y^{q^{r'}}, Z)$) est solution de $[b, q]_1$ (resp. de $[b, q]_2$) avec $UVW \neq 0$.*

3. Démonstrations pour $q \neq 2$

Réécrivons $[a, q]_1$ (resp. $[a, q]_2$) sous la forme

$$\Phi(a)(X/Y) = (Z/Y)^{q^r} \quad (\text{resp. } \Phi(a)(X/Y) = Z^p/(Y)^{q^r}),$$

avec $\Phi(a)x = ax + a_1x^q + \cdots + x^{q^r}$. On rappelle qu'on cherche une éventuelle solution avec $(X, Y) = 1$. Sans perte de généralité on suppose X et Y unitaires.

On a donc une équation:

$$(1)\qquad a(X/Y) + a_1(X/Y)^q + \cdots + a_{r-1}(X/Y)^{q^{r-1}} + (X/Y)^{q^r} = Z^e/(Y)^{q^r},$$

avec $e = q^r$ ou $e = p$. On dérive par rapport à T:

$$(2)\qquad a'(X/Y) + a_1'(X/Y)^q + \cdots + a_{r-1}'(X/Y)^{q^{r-1}} + a(X/Y)' = 0,$$

qui s'écrit encore

$$a'XY^{q^{r-1}-1} + a_1'X^qY^{q^{r-1}-q} + \cdots + a_{r-1}'X^{q^{r-1}} + aY^{q^{r-1}}(X/Y)' = 0.$$

Comme $Y^{q^{r-1}}(X/Y)' = (X'Y - XY')Y^{q^{r-1}-2}$ et que $a_{r-1}' \in (\mathbf{F}_q)^*$ (Lemme 1), dès que $q^{r-1} > 2$, Y doit diviser $X^{q^{r-1}}$ donc $Y = 1$.

On suppose maintenant $q \neq 2$. En reportant dans (1), on obtient

$$aX + a_1X^q + \cdots + a_{r-1}X^{q^{r-1}} + X^{q^r} = Z^e.$$

Le terme de gauche doit en particulier être une puissance p-ième. Comme d'après le Lemme 1, a_{r-1} est somme de T et de puissances p-ièmes, il faut aussi que

$$(3)\qquad aX + a_1X^q + \cdots + TX^{q^{r-1}},$$

soit une puissance p-ième. On utilise alors le Lemme 2 pour calculer le degré de $a_iX^{q^i}$: $\deg(a_iX^{q^i}) = q^i\deg(X) + q^i(r-i)$. Montrons que si $\deg(X) > 1$, le degré de l'expression (3) est celui de $TX^{q^{r-1}}$. Il suffit de vérifier que $q^{r-1}\deg(X)+1 > q^i\deg(X) + q^i(r-i)$, pour tout $0 \leq i \leq r-2$. Ce qui revient à l'inégalité:

$$q^{r-1}\deg(X) + 1 > q^{r-2}\deg(X) + 2q^{r-2},$$

ou

$$(q-1)\deg(X) > 2 - 1/q^{r-2}.$$

Comme $q \neq 2$, ceci est réalisé dès que $\deg(X) \geq 1$. Dans ce cas (3) est de degré $q^{r-1}\deg(X) + 1$ et ne peut donc pas être une puissance p-ième. On a donc également $X = 1$. L'équation (2) devient:

$$a' + a_i' + \cdots + a_{r-1}' = 0,$$

le Lemme 3 donne une contradiction si $r \geq 3$ ou si $r = 2$ et $p \neq 2$.

Il reste à examiner le cas $\deg(a) = 2$ et $p = 2$. Comme $q \neq 2$, les arguments précédents montrent que $X = 1$ et $Y = 1$. Comme a est unitaire, on aboutit à l'équation

$$a + a_1 + 1 = Z^e.$$

On écrit $a = T^2 + \alpha T + \beta$, on trouve $a_1 = T^q + T + \alpha$. L'équation devient

$$T^2 + \alpha T + \beta + T^q + T + \alpha + 1 = Z^e.$$

Si $e = q^2$ il est clair qu'il n'y a pas de solution. Les termes en T devant disparaître on a $\alpha = 1$. L'équation est donc

$$T^q + T^2 + \beta = Z^2;$$

il vient que β est aussi un carré. On a donc prouvé les Théorèmes 1, 2 et 3.

4. Le cas $q = 2$

Nous donnons des majorations du degré de X et de Y, indépendamment des preuves précédentes. Ce qui prouvera entièrement la Proposition 1.

a. **Preuve de la Proposition 1.** Supposons donné un triplet (X, Y, Z) de A^3 tel que $r = \deg(a) > 1$, $XYZ \neq 0$, $(X, Y) = 1$, $(Z, Y) = 1$ et (X, Y, Z) est solution de $[a, q]_1$ (resp $[a, q]_2$). Nous allons majorer $\deg(X)$ et $\deg(Y)$ ce qui suffit pour conclure.

Réécrivons $[a, q]_1$ (resp. $[a, q]_2$) sous la forme

$$\Phi(a)(X/Y) = (Z/Y)^{q^r} \quad (\text{resp: } \Phi(a)(X/Y) = Z^p/(Y)^{q^r}),$$

avec $\Phi(a)x = ax + a_1x^q + \cdots + a_rx^{q^r}$. On dérive par rapport à T (en se rappellant que $a_r \in \mathbf{F}_q$):

$$a'(X/Y) + a_1'(X/Y)^q + \cdots + a_{r-1}'(X/Y)^{q^{r-1}} + a(X/Y)' = 0,$$

qui s'écrit aussi

$$a'XY^{q^{r-1}-1} + a_1'X^qY^{q^{r-1}-q} + \cdots + a_{r-1}'X^{q^{r-1}} + aY^{q^{r-1}}(X/Y)' = 0.$$

En posant alors $\Psi(T) = (1/a)[a'F^0 + a_1'F + \cdots + a_{r-1}'F^{r-1}]$, le Lemme 1 dit que $a_{r-1}' \in (\mathbf{F}_q)^*$.

De plus, on peut donc appliquer le Lemme 2 qui affirme l'existence de $\hat{h}_\Psi$, tel qu'en appliquant $\hat{h}_\Psi$ dans l'égalité précédente on obtienne grâce au a) de ce même lemme:

$$q^{r-1}\hat{h}_\Psi(X/Y) \leq \hat{h}_\Psi((X'Y - XY')/Y^2).$$

Or le Lemme 2(b) implique

$$\hat{h}_\Psi((X'Y - XY')/Y^2) \leq h((X'Y - XY')/Y^2) + C_\Psi.$$

D'où l'on déduit (en utilisant $(X, Y) = 1$)

$$q^{r-1}\hat{h}_\Psi(X/Y) \leq 2h(X/Y) + C_\Psi \leq 2\hat{h}_\Psi(X/Y) + 3C_\Psi;$$

soit encore

$$(q^{r-1} - 2)\hat{h}_\Psi(X/Y) \leq 3C_\Psi. \tag{4}$$

Comme $q^{r-1} - 2 > 0$ et qu'il n'y a qu'un nombre fini de points de hauteur bornée, ceci conclut la preuve de la Proposition 1.

(b) **Conclusion du cas** $q = 2$. Comme $h(X/Y) \leq \hat{h}_\Psi(X/Y) + C_\Psi$, on tire de l'inégalité (4):

$$\max(\deg(X), \deg(Y)) \leq C_\Psi + 3C_\Psi/(q^{r-1} - 2).$$

D'après le Corollaire 1, on voit que la fonction de droite $f(r, q)$ est décroissante en r et en q on pourrait dans tous les cas obtenir de très bonnes majorations du degré de X. On regarde ici le cas $q = 2$. On obtient $f(3, 2) \leq 3, 4$; $f(4, 2) \leq 1, 8$; $f(r, 2) \leq 1, 8$ pour $r \geq 4$. Ceci implique $\deg(X) \leq 1$ dans tous les cas sauf le premier. Traitons donc maintenant les cas $\deg(a) > 3$.

On a $Y = 1$ et $\deg(X) \leq 1$: calculons $\Phi(a)(1)$. On remarque que $\Phi(T^2+T)(1) = 0$. On écrit la division euclidienne de a par $T^2 + T$: $a = R(T)(T^2+T) + eT + f$. Il vient,

$$\Phi(a)(1) = \Phi(R(T))\Phi((T^2+T))(1) + \Phi(eT+f)(1) = e(T+1) + f.$$

Pour que cette quantité soit un carré non nul (on rappelle $p = 2$), il est nécessaire et suffisant que $e = 0$ et $f = 1$.

Comme $\Phi(T)(T) = 0$, $\Phi(a)(T+g) = a(0)T + ge(T+1) + gf$. Si $a(0) = 1$, on trouve la même condition. Si T divise a, $f = 0$, il n'y a pas de solution. En conclusion si $r \geq 4$, il y a des solutions si et seulement si a est de la forme $a = R(T)(T^2+T) + 1$.

Remarque. Il y a des polynômes irréductibles de la forme $(T^2+T)b(T) + 1$, comme $T^3 + T^2 + 1$, $T^4 + T^3 + 1$, $T^6 + T^5 + 1$, ce qui montre qu'on obtient des solutions non réductibles en degré inférieur (cf. Lemme 7).

Passons maintenant au cas $\deg(a) = 3$. On va discuter l'équation inhomogène $([a, q]_2)$ et on en conclura les résultats correspondant pour l'équation homogène $([a, q]_1)$. L'équation est

$$aXY^7 + a_1X^2Y^6 + a_2X^4Y^4 + X^8 = Z^2,$$

on se demande donc si le terme de gauche peut être un carré. Ceci est équivalent au fait que $aXY^3 + a_1X^2Y^2 + a_2X^4$ soit un carré. Comme $a_2' = 1$ (Lemme 1), cette dernière assertion est équivalente au fait que $aXY^3 + a_1X^2Y^2 + TX^4$ soit un carré. Il faut donc que la dérivée soit nulle:

$$a'XY^3 + aX'Y^2 + aXY^2Y' + a_1'X^2Y^2 + X^4 = 0.$$

Mais alors tout facteur premier de Y divise X, donc $Y = 1$ (rappellons qu'on a supposé $(X, Y) = 1$). Il faut donc savoir si $aX + a_1X^2 + TX^4$ est un carré. Le degré de a est 3 et on vérifie que le degré de a_1 est 4. Ceci entraîne que si $\deg(X) > 1$, le degré de l'expression ci-dessus est $4\deg(X) + 1$, ce qui lui interdit d'être un carré. Le degré de X est donc ≤ 1. Reste à essayer les trois cas $X = 1$, T, $T + 1$. Un calcul montre qu'on trouve les solutions suivantes pour X (avec $Y = 1$):

$$T^3 + T^2 + T + 1: \quad X = 1,\ X = T + 1;$$

$$T^3 + T^2 + T: \quad X = 1,\ X = T,\ X = T + 1;$$

$$T^3 + T^2 + 1: \quad X = 1;$$

$$T^3 + T^2: \quad X = 1,\ X = T + 1;$$

$$T^3 + T + 1: \quad X = 1;$$

$$T^3 + T: \quad X = 1,\ X = T,\ X = T + 1;$$

$$T^3 + 1: \quad X = T + 1;$$

$$T^3: \quad X = T.$$

Voyons le cas $\deg(a) = 2$ pour $[a, q]_2$. Si $a = T^2 + 1$, $X = T + 1$ et $Y = T + b^2(T+1)$ (pour un b quelconque dans A) montre qu'il y a une infinité de solutions pour $[a, q]_2$. Si $a = T^2$, $X = T$ et $Y = 1 + b^2T$ donne le même résultat. Si $a = T^2 + T + 1$, on prend $X = T^2 + T + 1$, $Y = T + b^2$. Si $a = T^2 + T$, on prend $X = T^2 + T$, $Y = T + b^2$.

Enfin le cas homogène de degré 2 est plus subtil.

(a) $a = T^2$. L'équation est (a) $T^2XY^3 + (T^2 + T)X^2Y^2 + X^4 = Z^4$. Il est équivalent de dire que le terme de gauche doit être une puissance 4-ième. En particulier, $T^2XY + TX^2$, doit être un carré. Posons $Y/X = 1/T + A^2$. L'équation (a) a une solution si et seulement si $T^2(Y/X)^3 + (T^2 + T)(Y/X)^2$ est une puissance 4-ième. Ce qui donne $A^2 + T^2A^6 + T^2A^4$, qui est une puissance 4-ième uniquement si $A + TA^3 + TA^2$ est un carré. On écrit $A = U/V$ avec $(U, V) = 1$. Il est alors équivalent de dire que $UV^3 + TU^3V + TU^2V^2$ est un carré. Mais dans $\mathbf{F}_2[T]$ un élément est un carré si et seulement si sa dérivée est nulle:

$$U'V^3 + UV^2V' + U^3V + TU^2U'V + TU^3V' + U^2V^2 = 0,$$

d'où l'on tire que U divise $U'V^3$ et donc que $U' = 0$. Il vient

$$V^2V' + U^2V + TU^2V' + UV^2 = 0,$$

donc V divise TV'. Si $V' = 0$ on trouve $A = 1$. Sinon $V = TV'$ et on obtient $V = TU$, donc $A = 1/T$. Le cas $A = 1$ correspond à $(X, Y) = (T, T + 1)$ on trouve $Z = 0$, on a donc une solution triviale. Le cas $A = 1/T$ correspond à $(X, Y) = (T^2, T+1)$ et on trouve $Z = T$, on a donc une unique solution non triviale.

(b) $a = 1+T^2$. L'équation est (b) $(1+T^2)XY^3+(T^2+T+1)X^2Y^2+X^4 = Z^4$. Les solutions non triviales de cette équation sont exactement celles de l'équation précédente quand on change T en $T + 1$. Aussi obtient-on la seule solution: $(X, Y, Z) = (1 + T^2, T, T + 1)$.

(c) $a = 1+T+T^2$. L'équation est (c) $(1+T+T^2)XY^3+(1+T+T^2)X^2Y^2+X^4 = Z^4$. Il faut que le terme de gauche soit un carré donc que

$$a(Y/X) + a = c^2, \qquad c \in \mathbf{F}_2(T).$$

En reportant dans (c) on trouve que $c^6/a^2 + c^2$, doit être une puissance 4-ième, c'est à dire $c^3/a + c$, doit être un carré. On pose $c = U/V$. Il vient que $aU^3 + a^2UV^2$, doit être un carré, donc de dérivée nulle:

$$\text{(c}') \qquad a'U^3 + aU^2U' + a^2U'V^2 = 0.$$

D'où l'on tire que U^2 divise a^2U', ce qui entraîne $\deg U \leq 3$. Si a est premier avec U alors U divise U' donc $U' = 0$, on trouve $U = 0$, $X = 1$, $Y = 1$, $Z = 1$. Si a divise U, on écrit $U = aU_1$, en reportant dans (c′) et après simplification par a^2, on trouve

$$a'aU_1^3 + aU_1^2U' + U'V^2 = 0,$$

donc a divise $U' = a'U_1 + aU_1'$, donc $a = a'U_1$ ce qui contredit l'irréductibilité de a. En définitive la seule solution non triviale est $(X, Y, Z) = (1, 1, 1)$.

(d) $a = T + T^2$. L'équation est ici

$$\text{(d)} \qquad (T + T^2)XY^3 + (1 + T + T^2)X^2Y^2 + X^4 = Z^4.$$

Le terme de gauche est un carré donc on peut poser

$$(X/Y)(T + T^2) = T + C^2, \qquad C = U/V, \; C \in \mathbf{F}_2(T).$$

En reportant dans (d) il faut que $(Y/X)^2(C^2+1+T)^2$, soit une puissance 4-ième, c'est à dire que $(Y/X)(C+1+T)$, soit un carré, ou encore que le polynôme en U

et V suivant en soit un $VU^3T^2+V^2U^2T^3+VU^3T+U^2V^2T+T^3UV^3+T^2UV^3$. Sa dérivée est donc nulle:

$$V'U^3T^2 + VU'U^2T^2 + V^2U^2T^2 + V'U^3T + VU'U^2T + U^3V + U^2V^2 + T^2UV^3 + T^3U'V^3 + T^3UV'V^2 + T^2U'V^3 + T^2UV'V^2 = 0,$$

d'où V divise $V'(T+T^2)$ et U divise $U'(T^2+T^3)$. Comme $\deg V' \leq \deg V - 1$, et que U et V sont premiers entre eux, on a à examiner les cas:

$V = f(T+T^2)$ où f est un facteur de V' et $U' = 0$;
$V = V'T$ et U divise $U'(1+T)$;
$V = V'(T+1)$ et U divise $U'T^2$;
$V' = 0$ et U divise $U'(T^2+T^3)$.

Quelques calculs conduisent aux solutions non triviales: $(X, Y, Z) = (T^3, T^2+T+1, T^2+T)$; (T^3+1, T^2+T+1, T^2+T); $(1, T^2+T+1, T^2+T)$.

5. Fermat en dimension supérieure

Des généralisations intéressantes des modules de Carlitz ont été construites par Drinfeld (dimension 1, cf. [Dr]) et Anderson [A]. Comme me l'a fait remarquer D. Goss on peut définir l'équation de Fermat pour un t-module. Nous utiliserons la définition suivante (différente de celle de [A]):

Définition. Un t-module E, de dimension n est la donnée d'un couple $((\mathbf{G_a})^n, \Phi)$ où $(\mathbf{G_a})^n$ est le groupe additif de dimension n, Φ est un homomorphisme d'anneau injectif de $\mathbf{F}_q[t]$ dans $\mathrm{End}_{\mathbf{F}_q}((\mathbf{G_a})^n)$ déterminé par

$$\Phi(t) = a_0F^0 + \cdots + a_dF^d \quad (\text{où } F \text{ est le Frobenius}),$$

$a_0, \ldots, a_d \in \mathbf{M}_{n\times n}(\overline{k_\infty})$.

Rappelons quelques propriétés des hauteurs démontrées dans [D] (cf. Théorème 1). On se place maintenant dans un cadre algébrique: tous les a_i sont dans $\mathbf{M}_{n\times n}(\overline{k})$. On désigne par h la hauteur de Weil sur $(\mathbf{G_a})^n(\overline{k})$ et on suppose a_d inversible et $d \geq 1$. On utilise le théorème suivant.

Théorème A. *Il existe une unique fonction h_Φ: $(\mathbf{G_a})^n(\overline{k}) \to \mathbb{R}$, vérifiant:*

(1) *Pour tout $\alpha \in (\mathbf{G_a})^n(\overline{k})$ et tout $P \in \mathbf{F}_q[t]$, de degré r, $h_\Phi(\Phi(P)(\alpha)) = q^{dr}h_\Phi(\alpha)$.*

(2) *Il existe un réel $\gamma(\Phi)$ tel que $\gamma(\Phi) = \sup_{\alpha\in(\mathbf{G_a})^n(\overline{k})} |h(\alpha) - h_\Phi(\alpha)|$.*

(3) *Soit A une application de $(\mathbf{G_a})^n$ dans lui-même définie par des polynômes de degré $\leq D$. Il existe un réel $C_A > 0$ tel que pour tout $\alpha \in (\mathbf{G_a})^n(\overline{k})$, $h(A(\alpha)) \leq Dh(\alpha) + C_A$.*

Preuve. Les assertions (1) et (2) sont démontrées dans le Théorème 1 de [D]. La propriété (3) est prouvée dans [L, §3].

On se place maintenant sur E de dimension g. On note par des majuscules un g-uplet de $\mathbf{F}_q[T]$: $X = (x_1, \ldots, x_g)$. Pour a dans $\mathbf{F}_q[t]$, l'homomorphisme Ψ donné par $\Psi(t) = \Phi(a)$, définit un t-module. On désigne par q^d la puissance maximale à laquelle apparaît un x_i au moins.

On considère l'équation à $2g+1$ inconnues dans $\mathbf{F}_q[T]$:

$$(\Psi, q)\colon y^{q^d}\Phi(a)(X/y) = Z^p.$$

Ecrivons $\Psi(t) = a_0F^0 + \cdots + a_dF^d$, avec tous les $a_i \in \mathbf{M}_{n\times n}(\mathbf{F}_q(T))$. On définit le t-module Ψ' par $\Psi'(t) = a'_0F^0 + \cdots + a'_dF^d$ (où $'$ désigne la dérivation par rapport à T).

On se propose de montrer

Théorème 4. *On suppose que* a'_d *est inversible,* $d \geq 1$, $q^d > 2$. *Dans ces conditions* (Ψ, q) *a au plus un nombre fini de solutions vérifiant* $\mathrm{pgcd}(y, x_1, \dots, x_g) = 1$.

Remarque. Par homogénéïté, il est facile de voir que la condition

$$\mathrm{pgcd}(y, x_1, \dots, x_g) = 1$$

n'est pas restrictive.

Preuve. Il suffit de montrer qu'il y a au plus un nombre fini de $(g+1)$-uplets vérifiants $\mathrm{pgcd}(y, x_1, \dots, x_g) = 1$. Prenons donc une solution et dérivons par rapport à T, on obtient

$$a'_0(X/y) + \cdots + a'_d(X/y)^{q^d} = a_0((Xy' - X'y)/y^2).$$

On note $h_{\Psi'}$ la hauteur canonique de Ψ' qui existe car a'_d est inversible (Théorème A(1)). On prend la hauteur canonique de chaque membre de l'égalité précédente:

$$q^d h_{\Psi'}(X/y) = h_{\Psi'}(a_0((Xy' - X'y)/y^2)).$$

Puis,

$$q^d h_{\Psi'}(X/y) \leq h(a_0((Xy' - X'y)/y^2)) + \gamma(\Psi') \quad \text{(Théorème A(1), (2));}$$
$$q^d h_{\Psi'}(X/y) \leq C_{a_0} + 2h(X/y) + \gamma(\Psi') \quad \text{(Théorème A(3)).}$$

Enfin,

$$(q^d - 2)h_{\Psi'}(X/y) \leq C_{a_0} + 3\gamma(\Psi') \quad \text{(Théorème A(2)).}$$

Comme il n'y a qu'un nombre fini de points de hauteur bornée définis sur $\mathbf{F}_q[T]$, on a prouvé le théorème.

Une méthode similaire permet de montrer le même résultat de finitude dans les cas suivants.

Théorème 5.

1*er Cas.* $a'_d = 0$, a'_{d-1} *est inversible,* $d - 1 \geq 1$, $q^{d-1} > 2$.

2-*ième Cas.* a_d *est inversible dans* $M_{g\times g}(\mathbf{F}_q[T])$, $((a_d)^{-1})'' = 0$, $((a_d)^{-1}a_{d-1})''$ *est inversible,* $d - 1 \geq 1$, $q^{d-1} > 6$.

Preuve. Le premier cas se prouve de la même manière que le Théorème 4, on dérive par rapport à T et les hypothèses conduisent à remplacer d par $d-1$ dans la preuve précédente. Pour le second cas, on multiplie l'équation de départ par l'inverse de a_d puis on dérive deux fois.

Illustrons ce théorème par quelques exemples liés aux puissances tensorielles du module de Carlitz.

Définition (cf. [A.T.]). La puissance tensorielle g-ième du module de Carlitz est le t-module de dimension g déterminé par l'homomorphisme Φ_g tel que

$$\Phi_g(t)(x_1, \dots, x_g) = (Tx_1 + x_2, \dots, Tx_{g-1} + x_g, Tx_g + (x_1)^q).$$

Pour tout entier $k \geq 1$ il existe alors g polynômes à g variables $L_{1,k}, \ldots, L_{g,k}$ tels que

$$\Phi_g(t^k)(x_1, \ldots, x_g) = (L_{1,k}(x_1, \ldots, x_g), \ldots, L_{g,k}(x_1, \ldots, x_g)).$$

On peut alors écrire pour $1 \leq i \leq g$

$$L_{i,k}(x_1, \ldots, x_g) = \sum_{j=0}^{n} c_{i,j,k}\mathbf{w}_{i,j,k},$$

où $w_{i,j,k}$ est de la forme $(x_u)^{q^v}$, $1 \leq u \leq g$, $0 \leq v \leq [(k-1)/g] + 1$, les $w_{i,j,k}$ sont rangés dans l'ordre lexicographique croissant sur les couples (v, u) et les $c_{i,j,k}$ sont dans $\mathbf{F}_q[T]$. Avec cette convention, il est facile de voir qu'on a ainsi $c_{i,0,k} = T^k$, $c_{i,n,k} = 1$. On a vu dans [D] qu'on pouvait écrire

$$\Phi_g(t^g) = a_0F^0 + a_1F,$$

avec a_1 inversible, avec les notations précédentes, le fait que a_1 n'a que des 1 sur la diagonale se traduit par $w_{i,n,g} = (x_i)^q$.

Lemme 9. *Si* $k \geq g$, $1 \leq i \leq g$, $(c_{i,n-1,k})' = g - i + 1 \pmod p$.

Preuve. On a $c_{i,n-1,1} = T$ d'après la définition. Donc $(c_{i,n-1,1})' = 1$. Cette même définition permet d'établir la relation de récurrence:

$$c_{i,n-1,k+1} = Tc_{i,n,k} + c_{i+1,n-1,k} \quad \text{pour } 1 \leq i \leq g-1;$$
$$c_{g,n-1,k+1} = Tc_{g,n,k} + (c_{a,b,c})^q \quad \text{(on ne précise pas } a, b, c).$$

D'où l'on tire

$$(c_{i,n-1,k+1})' = 1 + (c_{i+1,n-1,k})' \quad \text{pour } 1 \leq i \leq g-1,$$
$$(c_{g,n-1,k+1})' = 1.$$

On conclut alors aisément, on a un tableau de cette forme

$$(i\backslash j) \quad \begin{matrix} 12344 \\ 12333 \\ 12222 \\ 11111 \end{matrix}$$

où le terme d'indice (i, j) est $(c_{i,n-1,j})'$, et où l'on construit un nouveau nombre en progressant en diagonale en ajoutant 1.

On va regarder l'équation de Fermat pour $\Phi_g(t^{gh+1}) = \Psi_h(t)$ et $h \geq 1$.

Corollaire. *On suppose que* $p > g$, $q^h > 2$. *Dans ces conditions* (Ψ_h, q) *a au plus un nombre fini de solutions vérifiant* $\operatorname{pgcd}(y, x_1, \ldots, x_g) = 1$.

Preuve. On peut écrire $\Phi_g(t^{gh}) = a_0F^0 + \cdots + a_hF^h$, avec a_h inversible ne possédant que des 1 sur la diagonale. Par composition avec $\Phi_g(t)$, on obtient

$$\Phi_g(t^{gh+1}) = b_0F^0 + \cdots + b_hF^h + b_{h+1}F^{h+1},$$

avec $(b_{h+1})' = 0$ et n'a que des termes nuls sur les diagonales supérieures d'ordre ≥ 2. D'après la forme de a_h la diagonale secondaire supérieure de b_h ne possède que des 1. De plus, la diagonale principale a pour coefficients $(c_{1,n-1,gh+1}, \ldots, c_{g,n-1,gh+1})$. Le Lemme 7 affirme alors que comme $p > g$, $(b_h)'$ est inversible. On peut donc appliquer le premier cas du Théorème 5.

Remarque. Un exemple d'application du second cas du théorème est donné par $\Phi_2(t^4)$, pour $p > 5$.

Le résultat du Théorème 4, pour un module de Drinfeld (en dimension 1 cf. [Dr]) est alors

Proposition 2. *Soit* $\Phi(t) = a_0F^0 + \cdots + a_dF^d$ *un t-module de dimension* 1 *défini sur* $\mathbf{F}_q(T)$ *et* h *le plus grand indice tel que* $a'_h \neq 0$. *On suppose* $h \geq 1$, $q^h - 2 > 0$, *alors l'équation* (Φ, q) *a au plus un nombre fini de solutions non triviales avec* $(X, Y) = 1$.

Remarque. La condition $h \geq 1$ est nécessaire. Considérons en effet un t-module donné par

$$\Phi(t) = T^pF^0 + a_1F + \cdots + a_{d-1}F^{d-1} + F^d;$$

où $a_i \in \{0, 1\}$ pour $1 \leq i \leq d-1$. L'équation

$$(\Phi, q)\colon y^{q^d}\Phi(t)(x/y) = z^p,$$

possède une infinité de solutions non triviales avec $x = T^{p^n - p}$ et $y = 1$, pour tout entier $n \geq 1$. Il est facile de généraliser cet exemple en dimension supérieure.

Comme D. Goss et D. Thakur me l'ont suggéré, la méthode permet d'aboutir à des énoncés de finitude dans une extension finie et séparable de $\mathbf{F}_q(T)$. On prouve le résultat suivant.

Proposition 3. *Soit* α *un élément algébrique séparable sur* k *et* $\Phi(t) = a_0F^0 + \cdots + a_dF^d$ *un t-module de dimension* 1 *défini sur* $k(\alpha)$. *Il existe un réel* $C_\alpha > 0$, *tel que si* $a'_d \neq 0$ *et* $q^d - C_\alpha > 0$, *alors l'équation* (Φ, q) *a au plus un nombre fini de solutions non triviales avec* $(X, Y) = 1$ *dans* $\mathbb{P}_1(k(\alpha))$.

Preuve. On part d'une solution éventuelle, on dérive comme précédemment, puis on prend la hauteur canonique. Il suffit ici pour conclure de montrer l'existence de réel a_α, b_α tels que pour tout $x \in k(\alpha)$, $h(x') \leq a_\alpha h(x) + b_\alpha$. Sur k on a vu $h(x') \leq 2h(x)$. On écrit alors chaque x sur la base $1, \alpha, \ldots, \alpha^u$: il existe $a_0, \ldots, a_u$ dans k tels que

$$x = \sum_{j=0}^{u} a_j\alpha^j. \tag{4}$$

On a donc

$$x' = \sum_{j=0}^{u}(a'_j\alpha^j + ja_j\alpha^{j-1}\alpha').$$

D'où l'on tire

$$h(x') \leq \sum_{j=0}^{u}(3h(a_j) + 2jh(\alpha)) + uh(\alpha').$$

Il reste alors à avoir pour chaque $0 \leq j \leq u$ une majoration $h(a_j) \leq eh(x) + f$ (avec $e, f > 0$). Si x, $\sigma_1(x), \ldots, \sigma_u(x)$ désignent les conjugués de x, on tire de la relation (4): $(x, \sigma_1(x), \ldots, \sigma_u(x)) = B(a_0, \ldots, a_u)$ où B est la matrice inversible de coefficients $(\sigma_i(\alpha^j))$. La propriété 3 du Théorème A permet de comparer la hauteur des deux $(u+1)$-uplets considérés:

$$h(a_0, \ldots, a_u) \leq h(x, \sigma_1(x), \ldots, \sigma_u(x)) + C_B.$$

Enfin, on remarque que $h(a_j) \leq h(a_0, \ldots, a_u)$ et $h(x, \sigma_1(x), \ldots, \sigma_u(x)) \leq (u+1)h(x)$, d'où l'on déduit une inégalité du type attendu:

$$h(x') \leq 3(u+1)^2 h(x) + C_\alpha.$$

RÉFÉRENCES

[A] G. Anderson, *t-motives*, Duke Math. J. **53** (1986), 457–502.

[A.T.] G. Anderson and D. Thakur, *Tensor powers of the Carlitz module and zeta values*, Ann. of Math. (2) **132** (1990), 159–191.

[D] L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), 213–223.

[Dr] V. G. Drinfeld, *Elliptic modules*, Math. USSR-Sb. **23** (1974), 561–592.

[G] D. Goss, *On a Fermat equation arising in the arithmetic theory of function fields*, Math. Ann. **261** (1982), 269–286.

[H] D. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

[L] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, Berlin and New York, 1983.

[M] R. C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Notes Ser. No. 96, Cambridge Univ. Press, London and New York.

[S] P. Samuel, *Lectures on old and new results on algebraic curves*, Tata Inst. Fund. Res., Bombay, 1966.

[V] J. V. Voloch, *A Diophantine problem on algebraic curves over function fields of positive characteristic*, Bull. Soc. Math. France **119** (1991), 121–126.

UNIVERSITÉ PIERRE ET MARIE CURIE, U.F.R. 920, 75252 PARIS, FRANCE

E-mail address: `ladenis@ccr.jussieu.fr`