JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Laurent DENIS

Facteurs communs et torsion en caractéristique non nulle

Tome 23, n° 2 (2011), p. 347-352.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_2_347_0>

Journal de Théorie des Nombres
de Bordeaux **23** (2011), 347-352

Facteurs communs et torsion en caractéristique non nulle

par Laurent DENIS

Résumé. Le pgcd de quantités de la forme $a^n - 1$ et $b^n - 1$ a été étudié dans différentes situations. Dans la première partie de ce texte nous prouverons que si a et b appartiennent à $\mathbb{F}_q[T]$, le pgcd en question peut être borné indépendamment de n dans de nombreux cas. Ceci répond en particulier à une question de J. Silverman. Dans la deuxième partie nous étudierons un problème analogue dans la situation des modules de Drinfeld.

Abstract. *Common factors and torsion in positive characteristic.*

The gcd of a^n-1 and b^n-1 has been studied in various setting. In the first part of that paper we show that if a and b are in $\mathbb{F}_q[T]$, there exist situations such that the degree of this gcd is bounded independently of n, this answer a question by J. Silverman. In the second part we will see what happens for an analogous problem concerning Drinfeld modules.

1. Résultats et situation

Si n est un entier naturel, le comportement du pgcd des quantités a^n-1 et b^n-1 a été étudié par différents auteurs selon l'anneau auquel appartiennent a et b.

Si a et b sont des entiers naturels plus grands que un et multiplicativement indépendants dans $\mathbb{Q}^*$, Bugeaud, Corvaja et Zannier prouvent dans [BCZ] que pour tout $\epsilon > 0$, il existe un entier $n_0(\epsilon, a, b)$ tel que si $n \geqslant n_0$, $\operatorname{pgcd}(a^n - 1, b^n - 1) \leqslant 2^{\epsilon n}$.

Si a et b sont des polynômes à coefficients complexes, multiplicativement indépendants dans $\mathbb{C}[T]^*$, Ailon et Rudnick démontrent dans [AR] qu'il existe un réel $c(a, b) > 0$ tel que $\deg \operatorname{pgcd}(a^n - 1, b^n - 1) \leqslant c(a, b)$.

Enfin si a et b appartiennent à un anneau de polynômes en une variable sur un corps à q éléments, Silverman montre au contraire que le pgcd est assez grand pour une infinité d'entiers n, plus précisément le résultat principal de [S] (theorem 4) est le suivant : pour tous a et b

Manuscrit reçu le 11 janvier 2010, révisé le 10 octobre 2010.
Classification math. 11T55, 11R58, 11D61.

unitaires dans $\mathbb{F}_q[T]$, pour tout entier k et $d \in \mathbb{Z}/q^k\mathbb{Z}$, il existe un réel $c(a,b,q^k) > 0$ et une infinité d'entiers n congrus à d modulo q^k tels que $\deg \operatorname{pgcd}(a^n - 1, b^n - 1) \geqslant c(a,b,q^k)n$.

Silverman demande s'il existe aussi une infinité d'entiers n pour lesquels le pgcd est borné. Dans cette note nous nous placerons sur un corps fini et donnerons dans une première partie la réponse (partielle) suivante à la question de Silverman :

Théorème 1.1. *Soit $\mathbb{F}_q[T]$ l'anneau des polynômes à coefficients dans le corps à q éléments de caractéristique p. On suppose que l'entier n est premier et que la classe de p engendre le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.*
a) Excepté le cas où on a à la fois $p = 2$ et 4 qui divise $n - 3$ on a :
pour tout a dans $\mathbb{F}_q[T] - \mathbb{F}_q$, $pgcd(a^n - 1, (a+1)^n - 1) = 1$ si $n > 2$ ou p différent de 3 et ce pgcd vaut $a - 1$ si $n = 2$ et $p = 3$.
b) On suppose p différent de 2 et on considère seulement des entiers naturels $D \geqslant 2$ premiers avec p. Si $\epsilon > 0$ alors il existe un entier q_0 dépendant de n, D et de ϵ tel que si $q > q_0$,

$$\operatorname{card}\left\{(a,b) \in \mathbb{F}_q[T]^2 \;\middle|\; \begin{array}{l} a \text{ et } b \text{ unitaires de degré } D \\ \deg(\operatorname{pgcd}(a^n - 1, b^n - 1)) \leqslant D \end{array}\right\} \geqslant (1-\epsilon)\frac{q^{2D}}{D^{2n-2}}.$$

Remarques. a) D'après le travail de Heath-Brown (voir [H-B]) sur la conjecture d'Artin, les conditions du théorème sont vérifiées pour une infinité d'entiers naturels premiers n sauf peut-être pour deux valeurs de p (et pour toutes les valeurs de p si la conjecture d'Artin est vraie).

b) Quand le pgcd vaut 1 pour une valeur première m de l'exposant alors par élévation des termes à la puissance p il vaut également 1 pour les valeurs $n = mp^s$.

c) Si $p = 2$ et 4 divise $n - 3$ dans la partie a) du théorème la situation est différente. Par exemple si $n = 3$ ou $n = 7$, le degré du pgcd est $n - 1$ alors que si $n = 11$ le pgcd reste 1.

Le résultat du b) viendra d'un théorème de Pollack sur l'hypothèse H de Schinzel sur $\mathbb{F}_q[T]$. On peut améliorer le terme en ϵ en suivant exactement l'énoncé obtenu par Pollack. On peut aussi obtenir un résultat de même nature si a et b sont de degrés différents (et de degré inférieur à D) de manière un peu plus rapide dans ce cas (voir la preuve du b) au paragraphe suivant).

Enfin dans la seconde partie, nous considérerons l'analogue du problème sur les modules de Drinfeld. On notera $k = \mathbb{F}_q(T)$, $k_\infty = \mathbb{F}_q((1/T))$ son complété pour la place à l'infini et $\overline{k_\infty}$ une clôture algébrique de k_∞.

Définition. Un module de Drinfeld de rang $d \geqslant 0$ sur $\mathbb{F}_q[T]$ est un homomorphisme injectif et $\mathbb{F}_q$-linéaire d'anneaux, $\Phi : \mathbb{F}_q[T] \to \operatorname{End}(G_a)$ tel que $\Phi(T) = T\mathbf{F^0} + ... + a_i\mathbf{F^i} + ... + a_d\mathbf{F^d}$ où $\mathbf{F}$ est le Frobenius relatif à

l'exposant q et a_d est non nul. Par la suite pour tout sous-anneau $\mathbb{A}$ de $\overline{k_\infty}$ on dira que Φ est défini sur $\mathbb{A}$ quand les $a_i (1 \leqslant i \leqslant d)$ appartiennent à $\mathbb{A}$. Pour N dans $\mathbb{F}_q[T]$-$\{0\}$ l'ensemble des zéros du polynôme $\Phi(N)(X)$ est celui des points de N-torsion du module de Drinfeld.

Comme $X^n - 1$ est le polynôme dont les racines sont les points de torsion d'ordre n du groupe multiplicatif, il est usuel de considérer $\Phi(N)(X)$ comme un analogue satisfaisant en caractéristique p de ce polynôme.

On dira que deux éléments A et B de $\overline{k_\infty}[z]$, sont Φ-indépendants si toute égalité du type $\Phi(N)(A) + \Phi(M)(B) = 0$ où N et M sont dans l'anneau des endomorphismes EndΦ du module de Drinfeld (on rappelle qu'il s'agit d'un $\mathbb{F}_q[T]$-module de type fini) entraîne $N = 0 = M$. C'est l'analogue de l'indépendance multiplicative de deux entiers.

Comme c'est souvent le cas en caractéristique p sur un groupe additif, cet analogue sur les modules de Drinfeld va s'avérer être beaucoup plus proche de la situation sur les corps de fonctions en caractéristique nulle que le précédent. On peut en fait se poser les deux questions suivantes :

Question 1. Si le module de Drinfeld est défini sur $\mathbb{F}_q[T]$ et que A et B sont des éléments de $\mathbb{F}_q[T]$, quel est le comportement en fonction de $N \in \mathbb{F}_q[T]$ de l'expression $\operatorname{pgcd}(\Phi(N)(A), \Phi(N)(B))$ dans $\mathbb{F}_q[T]$?

Question 2. Si le module de Drinfeld est défini sur $\overline{k_\infty}$ et que A et B sont des éléments de $\overline{k_\infty}[z]$, quel est le comportement en fonction de $N \in \mathbb{F}_q[T]$ de l'expression $\operatorname{pgcd}(\Phi(N)(A), \Phi(N)(B))$ dans $\overline{k_\infty}[z]$?

Les deux questions sont de nature différente. La question 1 plus arithmétique est liée à la notion de multiplication complexe du module de Drinfeld. Dans le cas d'un module de Carlitz $\Phi(T) = T\mathbf{F^0} + \mathbf{F}$, on sait par exemple que si N est irréductible N divise tous les coefficients de $\Phi(N)$ et donc notre pgcd n'est jamais borné. On va donc s'intéresser à la question 2 et voir qu'il s'agit du "bon analogue" du problème d'Ailon et Rudnick. Nous démontrerons le théorème suivant :

Théorème 1.2. *Soit A et B des éléments de $\overline{k_\infty}[z]$ supposés Φ indépendants alors il existe $H \in \mathbb{F}_q[T] - \{0\}$ tel que pour tout N dans $\mathbb{F}_q[T]$-$\{0\}$, $\operatorname{pgcd}(\Phi(\mathrm{N})(\mathrm{A}), \Phi(\mathrm{N})(\mathrm{B}))$ divise H.*

Remarques. Au vu de ce résultat il pourrait être intéressant de formuler (et de prouver) un résultat similaire sur les courbes elliptiques.

2. Preuve des théorèmes

2.1. Le théorème 1.1. Commençons par le a) du théorème 1.1, et plus précisément par le cas $a = T$ qui est d'ailleurs le cas particulier fondamental déjà étudié dans [S]. On a la décomposition $T^n - 1 = (T-1)(1 + T + \cdots + T^{n-1})$. Nous supposerons maintenant que n est un nombre premier ; alors

on reconnaît le polynôme cyclotomique d'ordre n, $\Phi_n(T) = 1 + T + \cdots + T^{n-1}$. Si $n = 2$ la propriété énoncée au a) est vraie, nous supposerons donc $n > 2$. Le polynôme $\Phi_n(T)$ est irréductible sur $\mathbb{F}_p$ s'il n'a aucune racine dans une extension quelconque de $\mathbb{F}_p$ de degré $j \leqslant (n-1)/2$, c'est-à-dire aucune racine dans $\mathbb{F}_{p^j}$ pour tout tel j. Soit ξ une racine de $\Phi_n(T)$ dans une extension suffisamment grande de $\mathbb{F}_p$. Dès que n est premier et différent de p, ξ est une racine n-ième de l'unité d'ordre exactement n. Elle appartient à $\mathbb{F}_{p^j}^*$ si et seulement si n divise $p^j - 1$ d'où l'irréductibilité de $\Phi_n(T)$. En substituant $T + 1$ à T on a aussi l'identité $(T+1)^n - 1 = T\Phi_n(T+1)$ et sous les hypothèses précédentes on a écrit la décomposition en facteurs irréductibles de ce polynôme. Par conséquent $\mathrm{pgcd}(T^n - 1, (T+1)^n - 1)$ a comme facteurs premiers éventuels T, $T-1$, $\Phi_n(T)$ et $\Phi_n(T+1)$. Il est clair que ni T ni $T-1$ ne divisent ce pgcd. Reste à voir si $\Phi_n(T)$ divise ce pgcd, cela ne se produit que si $\Phi_n(T) = \Phi_n(T+1)$. La comparaison des termes de degré inférieur ou égal à 1 de ces polynômes fournit $n = 1$ modulo p, puis $n(n-1)/2 = 1$ modulo p. Si p est impair, c'est absurde. Si $p = 2$, mais que 4 divise $n - 1$, c'est également absurde.

Si on écrit alors une relation de Bezout entre $T^n - 1$, $(T+1)^n - 1$ et leur pgcd, alors en spécialisant T en $a(T)$, on en déduit immédiatement le a).

Traitons maintenant le b) du théorème 1.1. Rappelons avec nos notations le "theorem A" de Pollack (voir [P]) :

Theorem A. *Soit $(f_1, ..., f_r)$ un r-uplet de polynômes irréductibles non associés de $\mathbb{F}_q[T]$ tel que $\deg(\prod_{1\leqslant i\leqslant r} f_i) \leqslant B$. Alors si les entiers $2D$ sont premiers à p on a :*

$$\mathrm{card}\left\{ \mathrm{g} \;\middle|\; \begin{array}{l} g \text{ unitaire de degré } D \\ f_1(g(T)), \ldots, f_r(g(T)) \text{irréductibles} \end{array} \right\} \geqslant \frac{\mathrm{q}^{\mathrm{D}}}{\mathrm{D}^{\mathrm{r}}} + \mathrm{O}_{\mathrm{D,B}}(\mathrm{q}^{\mathrm{D}-1/2}).$$

Sous nos hypothèses on peut écrire :

$$a(T)^n - 1 = (a(T) - 1)\Phi_n(a(T)) \text{ et } b(T)^n - 1 = (b(T) - 1)(\Phi_n(b(T)).$$

Pour conclure la preuve il suffit donc de prouver qu'aucun facteur irréductible de $\Phi_n(a(T))$ ou de $\Phi_n(b(T))$ ne divise le pgcd qu'on cherche à décrire quand a et b sont bien choisis et de degré D.

Si ξ est une racine primitive n-ième de l'unité, elle engendre un corps $\mathbb{F}_{q^m} = \mathbb{F}_q(\xi)$ où m est l'ordre de q modulo n. On a $\Phi_n(T) = \prod_{1\leqslant i\leqslant n-1} (T - \xi^i)$.

Ecrivons la décomposition en facteurs irréductibles unitaires de $\Phi_n(T)$ sur $\mathbb{F}_q$: $\Phi_n(T) = \prod_{1\leqslant i\leqslant r} P_i(T)$, les racines de chaque polynôme P apparaissant dans cette décomposition sont des puissances de ξ et si ξ^j est une racine de P alors ses autres racines sont de la forme ξ^{jq^s} (pour un certain entier s). Comme n est premier, on voit facilement que tous les polynômes P_i de la décomposition précédente sont de degré m.

Rappelons brièvement que si F est un polynôme irréductible de degré $m = \deg F$ sur $\mathbb{F}_q[T]$ et que G appartient à $\mathbb{F}_q[T]$ alors le composé $F(G)$ est irréductible sur $\mathbb{F}_q[T]$ si et seulement s'il existe une racine λ de F telle que $G(T)-\lambda$ soit irréductible sur $\mathbb{F}_{q^m}[T]$. En effet une racine x de $F(G)(T)$ va être algébrique de degré $\deg F.\deg G$ sur $\mathbb{F}_q$ si et seulement si pour au moins une racine λ de F, $G(T)-\lambda$ est associé au polynôme minimal de x sur $\mathbb{F}_{q^m}$.

On applique alors le theorem A aux polynômes $P_1, ..., P_r$ dont le produit est de degré $n-1$ et on choisit a et b de degré D tels que tous les $P_i(a(T))$ et $P_i(b(T)), (1 \leqslant i \leqslant r)$ soient irréductibles sur $\mathbb{F}_q$, on a donc l'existence d'entiers i_1, i_2 compris entre 1 et $n-1$ tels que $a(T)-\xi^{i_1}$ et $b(T)-\xi^{i_2}$ soient irréductibles sur $\mathbb{F}_{q^m}$. Mais si pour un entier i_1 le polynôme $a(T)-\xi^{i_1}$ est irréductible alors par action du groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ (en utilisant cette action pour chaque polynôme P_i) tous les polynômes $a(T)-\xi^l$ pour $1 \leqslant l \leqslant n-1$ sont irréductibles sur $\mathbb{F}_{q^m}$ et de même pour les polynômes $b(T)-\xi^l$. Pour qu'un facteur irréductible sur $\mathbb{F}_q[T]$ soit commun à $\Phi_n(a(T))$ et à $\Phi_n(b(T))$ il faut donc qu'on ait une égalité $P_i(a(T)) = P_j(b(T))$ et donc une égalité $a(T)-\xi^u = b(T)-\xi^v$ (pour certains entiers u, v). Ceci est évité dès que $a(T)-b(T)$ n'est pas un élément de $\mathbb{F}_q$. Le cardinal des couples $(a(T), b(T))$ qui vérifient $a(T)-b(T) \in \mathbb{F}_q$, avec des composantes unitaires de degré D est q^{D+1}. On ne considère alors que les couples $(a(T), b(T))$ dont les deux coordonnées apparaissent dans le theorem A et qui vérifient $a(T)-b(T) \notin \mathbb{F}_q$, avec ces précautions $\mathrm{pgcd}(\Phi_n(a(T)), \Phi_n(b(T)) = 1$. Si $m > 1$, un facteur irréductible de $\Phi_n(a(T))$ est de degré mD et ne peut pas non plus diviser $b(T)-1$. On a donc $\deg \mathrm{pgcd}(a^n-1, b^n-1) \leqslant \deg(a-1) \leqslant D$. Enfin si $m = 1$ ceci implique qu'on a un $a(T)-\xi^{i_1}$ irréductible sur $\mathbb{F}_q$ et on arrive facilement à la même conclusion quand $a(T)-b(T) \notin \mathbb{F}_q$. Comme $r \leqslant n-1$, le cardinal des couples désirés dans le théorème 1.1,b) est donc supérieur à $(\frac{q^D}{D^{n-1}} + O_{D,B}(q^{D-1/2}))^2 - q^{D+1}$ d'où le résultat.

2.2. Le théorème 1.2. Regardons pour commencer le cas dégénéré $d = 0$, module à action dite triviale. Dans ce cas $\mathrm{pgcd}(\Phi(N)(A), \Phi(N)(B)) = \mathrm{pgcd}(NA, NB) = N\mathrm{pgcd}(A, B)$ ne dépend pas de N dans $\overline{k_\infty}[z]$. Par la suite nous supposerons $d > 0$ et conserverons les notations du théorème 1.2.

Tout comme dans la preuve d'Ailon et Rudnick nous utiliserons un théorème à la "Manin-Mumford". Dans le cadre des modules de Drinfeld la preuve de ce théorème est due à Scanlon [Sc]. En particulier ce dernier prouve qu'une courbe irréductible C du plan affine ne peut rencontrer une infinité de points de torsion du produit direct $\Phi \times \Phi$ de deux modules de Drinfeld que si C est la translatée d'un sous-T-module par un point de torsion.

L'équation d'un sous-T-module de dimension un de $\Phi \times \Phi$ est de la forme $\Phi(Q)(X) + \Phi(R)(Y) = 0$ où Q et R appartiennent à EndΦ (voir par exemple l'appendice de [T]). Donc l'équation d'un translaté par un point de torsion est $\Phi(Q)(X) + \Phi(R)(Y) + \xi = 0$ où ξ est un point de torsion du module de Drinfeld. Par conséquent si $A(z)$ et $B(z)$ sont Φ-indépendants, $\{(A(z), B(z)) \,|\, z \in \overline{k_\infty}\}$ est une courbe irréductible du plan affine qui ne contient qu'un nombre fini de points de torsion de $\Phi \times \Phi$. Ainsi $S = \{s \in \overline{k_\infty}/(A(s), B(s)) \text{ est un point de torsion}\}$ est un sous-ensemble fini de $\overline{k_\infty}$.

Donc $\text{pgcd}(\Phi(N)(A(z)), \Phi(N)(B(z))) = \prod_{s\in S}(z-s)^{e(s)}$ où $e(s)$ est un entier naturel. Or $\Phi(N)(A(z)) = c(N)\prod_{x\in Ker\Phi(N)}(A(z)-x)$ où $c(N)$ est dans $\overline{k_\infty}$. Comme les racines de $\Phi(N)$ sont simples, si $z-s$ apparaît dans le pgcd cherché, il existe un unique x dans le noyau de $\Phi(N)$ tel que $z-s$ divise $A(z)-x$ et pour des raisons de degré $e(s) \leqslant \deg(A)$. Il suffit donc de prendre $H(z) = \prod_{s\in S}(z-s)^{min(\deg A, \deg B)}$ pour achever la preuve du théorème 1.2.

Remarques. L'analogue des compléments prouvés par Ailon et Rudnick peut aussi être traité et est laissé au lecteur (voir [AR]).

Remerciements. L'auteur remercie vivement l'arbitre pour lui avoir signalé une erreur et avoir grandement contribué à la clarté de cet article.

Bibliographie

[AR] N. Ailon, Z. Rudnick, *Torsion point on curves and common divisors of $a^k - 1$ and $b^k - 1$.* Acta. Arithmetica **113 :1** (2004), 31–38.

[BCZ] Y. Bugeaud, P. Corvaja, U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$.* Math. Zeit. **243 :1** (2003), 79–84.

[H-B] D.R. Heath-Brown, *Artin's conjecture for primitive roots.* Quart. J. Math. Oxford Ser (2) **37** (1986), 27–38.

[P] P. Pollack, *An explicit approach to hypothesis H over a finite field.* À paraître dans : The anatomy of integers. Proceedings of a conference on the anatomy of integers, Montreal, March 13th-17th, 2006, eds : J.M. de Koninck, A. Granville and F. Luca.

[Sc] T. Scanlon, *Diophantine geometry of the torsion of a Drinfeld module.* Journal of number theory **97 :1** (2002), 10–25.

[S] J. Silverman, *Common divisors of $a^n - 1$ and $b^n - 1$ over function fields.* New York Journal of Mathematics **10** (2004), 37–43.

[T] A. Thiery, *Théorème de Lindemann-Weierstrass pour les modules de Drinfeld.* Compositio Math. **95 :1** (1995), 1–42.

Laurent Denis
Université des sciences et technologies de Lille
Batiment M2
59655 Villeneuve d'ascq Cedex
E-mail: Laurent.Denis@math.univ-lille1.fr