PUB. IRMA, LILLE 2010
Vol. 70, N° II

Facteurs communs et torsion en caractéristique non nulle

Laurent Denis

Laboratoire Paul Painlevé, UMR 8524
UFR de Mathématiques, USTL, Bât. M2
59655 Villeneuve d'Ascq Cedex France

Article déposé le 12 novembre 2009

Abstract

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.

Résumé

Le pgcd des quantités a^n-1 et b^n-1 a été étudié dans des cadres variés. Dans la première partie de cet article nous montrerons que si a et b sont dans $\mathbb{F}_q[T]$, il existe des situations où le pgcd est borné indépendamment de l'entier n, répondant en cela à une question de J. Silverman. Dans une seconde partie nous examinerons un problème analogue en liaison avec les modules de Drinfeld.

MSC 2000 subject classifications. 11T55, 11R58, 11D61.

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 di□érents 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 que pour tout $\varepsilon > 0$, il existe un entier $n_0(\varepsilon, a, b)$ tel que si $n \geq n_0$, pgcd$(a^n - 1, b^n - 1) \leq 2^{\varepsilon n}$.

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

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 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 pgcd$(a^n - 1, b^n - 1) \geq c(a, b, q^k)n$.

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. *Soit $\mathbb{F}_q[T]$ l'anneau des polynômes à coe cients 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 :
pgcd$(T^n - 1, (T + 1)^n - 1) = 1$ *si* $n > 2$ *ou* $p \neq 3$ *et ce pgcd vaut* $T - 1$ *si* $n = 2$ *et* $p = 3$.

b) Excepté le cas où on a à la fois $p = 2$ et 4 qui divise $n - 3$ on a :
pour tout a dans $\mathbb{F}_q[T] \setminus \mathbb{F}_q$, pgcd$(a^n - 1, (a + 1)^n - 1) = 1$ *si* $n > 2$ *ou* $p \neq 3$ *et ce pgcd divise* $a - 1$ *si* $n = 2$ *et* $p = 3$.

c) On suppose $p \neq 2$ et on considère uniquement des entiers naturels D premiers avec $2p$. Si $\varepsilon > 0$, alors il existe un entier q_0 dépendant de n, D et de ε tel que si $q > q_0$,

$$\text{card}\left\{(a, b) \in \mathbb{F}_q[T]^2 \text{ unitaires de degré } D \mid \deg\left(\text{pgcd}(a^n - 1, b^n - 1)\right) \leq 2D\right\} \geq (1 - \varepsilon)\frac{q^{2D}}{D^2}.$$

Remarques. a) D'après le travail de Heath-Brown [H-B] sur la conjecture d'Artin, les conditions du théorème 1 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 $n-3$, la situation est di□érente. Par exemple si n = 3 ou n = 7, le degré du pgcd est $n-1$ alors que si n = 11 le pgcd reste 1.

d) Le résultat du c) 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 di□érents (et de degré inférieur à D) de manière un peu plus rapide dans ce cas (voir la preuve du c) 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_∞ = $\mathbb{F}_q((1/T))$ son complété pour la place à l'infini, $\overline{k_\infty}$ une clôture algébrique de k_∞ et $\overline{k}$ l'ensemble de ses éléments algébriques sur k.

Definition 1. Un module de Drinfeld de rang $d \geq 0$ sur $\mathbb{F}_q[T]$ est un homomorphisme injectif d'anneau $\Phi : \mathbb{F}_q[T] \to \mathrm{End}(G_a)$ tel que $\Phi(T) = T\mathsf{F}^0 + a_1\mathsf{F} + \cdots + a_d\mathsf{F}^d$ où F est le Frobenius relatif à l'exposant q.

On dira par la suite que Φ est défini sur le sous-anneau A de $\overline{k_\infty}$, si les a_i ($1 \leq i \leq d$) appartiennent à A.

Pour N dans $\mathbb{F}_q[T] \setminus \{0\}$, l'ensemble des zéros du polynôme $\Phi(N)(X)$ sont 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 $\overline{k_\infty}$, sont Φ-indépendants si toute égalité du type $\Phi(N)(A) + \Phi(M)(B) = 0$ où N et M sont dans l'anneau des endomorphisrnes $\mathrm{End}\,\Phi$ 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 si 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 $\mathrm{pgcd}(\Phi(N)(A), \Phi(N)(B))$ dans $\mathbb{F}_q[T]$?

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

Les deux questions sont de nature di□érente. 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 $\Phi(T) = T\mathsf{F}^0 + \mathsf{F}$, on sait par exemple que si N est irréductible, N divise tous les coe□cients 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 montrerons le théorème suivant.

Théorème 2. *Soit A et B des éléments de $\mathbb{F}_q[z]$ supposés Φ-indépendants et N dans $\mathbb{F}_q[T] \setminus \{0\}$. Alors il existe $H \in \mathbb{F}_q[T]$ tel que* pgcd($\Phi(N)(A), \Phi(N)(B)$) *divise H.*

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

2 Preuves des théorèmes

2.1 Le théorème 1

Commençons par le a) du théorème 1, il s'agit du 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 $j \leq (n-1)/2$, 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 a $\mathbb{F}_{p^j}^*$ si et seulement si n divise $p^j - 1$ d'où l'irréductibilité de $\Phi(T)$. 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 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 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 b).

Enfin pour le c) du théorème, rappelons avec nos notations le theorem A de Pollack (voir [P]) dans le cas d'un seul polynôme irréductible.

Theorem A (Pollack). *Soit f polynôme irréductible sur $\mathbb{F}_q[T]$, de degré inférieur à B, alors si les entiers D sont premiers à $2p$, on a :*

$$\text{card}\{g \text{ unitaires de degré } D \text{ tels que } f(g(T)) \text{ est irréductible}\} \geq \frac{q^D}{D} + O_{D,B}(q^{D-1/2}).$$

Alors sous nos hypothèses $a(T)^n - 1 = (a(T) - 1)\Phi_n(a(T))$ et $b(T)^n - 1 = (b(T) - 1)\Phi_n(b(T))$ où $\Phi_n(T)$ est irréductible sur $\mathbb{F}_q[T]$. Pour conclure la preuve, il suffit de prouver que $\Phi_n(a(T))$ et $\Phi_n(b(T))$ ne peuvent diviser le pgcd qu'on cherche à décrire. Grâce au théorème de Pollack on choisit a et b tels que $\Phi_n(a(T))$ et $\Phi_n(b(T))$ soient tous les deux irréductibles.

Rappelons brièvement que si F est un polynôme irréductible de degré $d = \deg F$ sur $\mathbb{F}_q[T]$ et si 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 $\mathbb{F}_{q^d}[T]$. En effet une racine x de $F(G)(T)$ va être algébrique de degré $\deg F \cdot \deg G$ 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 $\mathbb{F}_{q^d}$.

Avec ici $F = \Phi_n$ et $G = a$ ou b, on a donc sous les hypothèses précédentes que $a(T) - \xi^i$ et $b(T) - \xi^j$ sont irréductibles sur $\mathbb{F}_{q^{n-1}}[T]$ pour des entiers i et j compris entre 1 et $n-1$ et ξ une racine primitive n-ième de 1 (rappelons que n et p sont différents) dans $\mathbb{F}_{q^{n-1}}$. Mais si pour un tel entier i, le polynôme $a(T) - \xi^i$ est irréductible, alors par action du groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^{n-1}}/\mathbb{F}_q)$, tous les polynômes $a(T) - \xi^i$ pour $1 \leq i \leq n-1$ sont irréductibles sur $\mathbb{F}_{q^{n-1}}[T]$ et de même pour $b(T) - \xi^i$. Or si $\Phi_n(a(T)) = \Phi_n(b(T))$, alors ces polynômes unitaires se décomposent en $\prod_{1\leq i\leq n-1}(a(T) - \xi^i) = \prod_{1\leq i\leq n-1}(b(T) - \xi^i)$, par conséquent $a(T)$ et $b(T)$ diffèrent uniquement par une constante appartenant à $\mathbb{F}_q$. Le cardinal de l'ensemble des couples $(a(T), b(T))$ tels que $\Phi_n(a(T)) = \Phi_n(b(T))$ qui apparaissent dans le theorem A précédent est donc majoré par un $O(\frac{q^D}{D})$, d'où le résultat.

2.2 Le théorème 2

Regardons pour commencer le cas dégénéré $d = 0$, module à action dite triviale, alors $\mathrm{pgcd}(\Phi(N)(A), \Phi(N)(B)) = \mathrm{pgcd}(N(A), N(B)) = N\,\mathrm{pgcd}(A, B)$ ne dépend pas de N dans $\overline{\mathsf{k}_\infty}[z]$. Par la suite nous supposerons $d > 0$ et conserverons les notations du théorème 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 T. 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.

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 $\mathrm{End}\,\Phi$ (voir par exemple [D]). 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, $\{(a(z), b(z)) \mid z \in \overline{\mathsf{k}_\infty}\}$ est une courbe irréductible du plan affine qui ne contient qu'un nombre fini de points de torsion de $\Phi \times \Phi$. Ainsi il existe un sous-ensemble fini S de $\overline{\mathsf{k}_\infty}$ tel que pour tout s dans S, $A(s)$ et $B(s)$ sont des points de torsion.

Donc $\mathrm{pgcd}\left(\Phi(N)(A(z)), \Phi(N)(B(z))\right)$ divise $\prod_{s\in S}(z - s)^{e(s)}$ 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 $e(s) \leq \deg(A)$. Il su□t donc de prendre $H(z) = \prod_{s\in S}(z-s)^{\max(\deg A,\deg B)}$ pour achever la preuve du théorème 2.

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

Références

[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.

[D] L. Denis, Théorème de Baker et modules de Drinfeld, *J. Number Theory*, **43**(1993), 203–215.

[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.