Astérisque

YVETTE AMICE
BRUNO KAHN

Sommes de puissances dans les corps finis

Astérisque, tome 209 (1992), p. 115-135
<http://www.numdam.org/item?id=AST_1992__209__115_0>

Sommes de puissances dans les corps finis

Yvette Amice et Bruno Kahn

Introduction

Soit F un corps fini à q éléments, où q est une puissance d'un nombre premier impair. On note $s(q)$ le plus petit entier s tel que -1 soit somme de s éléments de F* d'ordre (multiplicatif) impair. L'étude de cet entier est motivée par celle des "niveaux supérieurs" d'un corps (§1).

Le but de cet article est de présenter et de commenter le calcul de $s(q)$ pour q premier $< 10^9$ et $q = p^3$ avec p premier $\leq 101\ 711\ 783$ (pour $q = p^n$ avec p premier et $n \neq 1, 3$, on a $s(q) = 2$, *cf* prop. 1, 4)). L'intérêt principal de cette présentation est que les résultats obtenus offrent des caractéristiques inattendues à plusieurs égards. Pour résumer ces caractéristiques, on peut dire qu'en général $s(q)$ est "plus petit" qu'on ne pourrait s'y attendre.

Le paragraphe 1 rappelle la définition des niveaux supérieurs d'un anneau. Les paragraphes 2 et 3 donnent des résultats généraux sur l'entier $s(q)$, notamment les majorations qui ont été utilisées dans les calculs. Le paragraphe 4 décrit les résultats obtenus, et en particulier une série de "phénomènes inexpliqués". Le paragraphe 5 donne quelques questions ouvertes. Enfin, une annexe contient 10 tables extraites de nos calculs, qui illustrent les descriptions données au paragraphe 4.

1. Niveaux supérieurs d'un anneau

Soit A un anneau commutatif de caractéristique différente de 2. Pour tout entier $r \geq 1$, on notera suivant Revoy [R] $s_r(A)$ le plus petit entier s tel que l'équation $-1 = x_1^{2^r} + \ldots + x_s^{2^r}$ ait une solution dans A (ou ∞ si un tel entier n'existe pas). Ainsi, si A est un corps F, $s_1(F)$ n'est autre que le niveau de F étudié notamment par Pfister ([P1], [P2]); $s_2(F)$ a été étudié entre autres dans [PAR1], [PAR2]. Les nombres $s_r(A)$ ont les propriétés évidentes suivantes:

(A) Si A→A' est un homomorphisme d'anneaux, $s_r(A) \geq s_r(A')$.

(B) Si ℓ est un nombre premier impair tel que A contienne une racine primitive ℓ–ième de l'unité ζ telle que $\zeta-1$ ne soit pas diviseur de zéro, on a $s_r(A) \leq \ell-1$ pour tout $r \geq 1$ ([R], prop. 1.6).

L'étude des $s_r(F)$ pour les corps finis est intéressante, d'un part en soi, d'autre part pour les informations qu'elle donne sur les s_r des corps de nombres ([PAR1], [PAR2], [R]).

2. Cas des corps finis: résultats "théoriques"

Supposons que F soit un corps fini à q éléments (q impair); soit $h = h(q)$ le plus grand entier tel que 2^h divise $q-1$. On a alors ([R], th. 2.2):

a) $s_r(F) = 1$ si $r < h$;

b) $1 < s_h(F) = s_r(F) \leq 2^h$ si $r \geq h$.

On note $s(F)$, ou simplement $s(q)$, l'entier $s_h(F)$. Pour un entier s, les conditions suivantes sont équivalentes:

(i) $s \geq s(q)$;

(ii) -1 est somme de s éléments de F, nuls ou d'ordre (multiplicatif) impair;

(iii) l'hypersurface projective d'équation $X_0^{2^h}+\ldots+X_s^{2^h} = 0$ a un point F–rationnel.

La proposition suivante donne quelques renseignements sur le comportement de $s(q)$ en fonction de q. Soit p la caractéristique de F, de sorte que q est une puissance de p.

|| **Proposition 1.** 1) *Si* $\frac{\sqrt{q}^n-\sqrt{q}^{-n}}{\sqrt{q}-\sqrt{q}^{-1}} > (1-2^{-h})[(2^h-1)^n-(-1)^n]$, *on a* $s(q) \leq n$; *en particulier, si* $q \geq 2^{2nh/(n-1)}$, *on a* $s(q) \leq n$.

2) *Si* $q \geq (2^h-1)^2(2^h-2)^2$, *on a* $s(q) = 2$.

3) *Si* $q \geq (2^h-1)(2^{2h}-3\cdot 2^h+3)$, *on a* $s(q) \leq 3$.

4) *Si q n'est pas de la forme p ou* p^3, *on a* $s(q) = 2$.

5) *Si* $q = p^3$, on a $s(q) \leq 3$. *On a* $s(q) = 2$, *sauf peut-être si* $s(p) > 2$ *et* $p < 2^{4h/3}$.

6) *Si p est un nombre premier de Fermat, on a* $s(p) = p-1$.

Démonstration. 6) est évident (*cf* [R], 2.4), et 2) et 3) sont des cas particuliers de 1) (pour 2), *cf* [R] , dém. du lemme 2.3). Supposons $q = p^n$. Si n

est pair, $q-1$ est divisible par 3 donc $s(q) \leq 2$ d'après la propriété (B) rappelée ci-dessus, d'où $s(q) = 2$. Si n est impair, on a $h(q) = h(p)$; si $n \geq 5$, on a donc $q \geq p^5 \geq 2^{5h} \geq 2^{4h}$, d'où $s(q) = 2$ d'après 1); cela démontre 4). En notant que de même 5) est conséquence de 1), il reste à démontrer 1). Pour cela, on minore le nombre de points rationnels de l'hypersurface projective $X_0{}^{2^h}+\ldots+X_n{}^{2^h} = 0$. Une telle minoration peut bien sûr se déduire des conjectures de Weil démontrées par Deligne, mais on peut aussi procéder directement au moyen de sommes de Jacobi généralisées, en reprenant les arguments de Weil, *cf* [L], *pp.* 22–24. Plus généralement, soient d un diviseur de $q-1$ et Y_n l'hypersurface *affine* d'équation $X_0{}^d+\ldots+X_n{}^d = 0$. En suivant Lang (*op. cit.*), on voit que le nombre de points F-rationnels de Y_n est:

$$E_n = \sum_{(a_0,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z})^{n+1}} \sum_{u_0+\ldots+u_n=0} \chi^{a_0}(u_0)\ldots\chi^{a_n}(u_n),$$

où χ est un caractère multiplicatif fixé, d'ordre d. En transformant cette équation comme dans [L] (*loc. cit.*), on trouve:

$$E_n = q^n-(q-1) \sum_{\substack{(a_1,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z}-\{0\})^n \\ a_1+\ldots+a_n\neq 0}} \chi^{a_1+\ldots+a_n}(-1)\, J(\chi^{a_1},\ldots,\chi^{a_n}),$$

où $J(\chi_1,\ldots,\chi_n) = -\sum_{x_1+\ldots+x_n=1} \chi_1(x_1)\ldots\chi_n(x_n)$ est une somme de Jacobi généralisée. Le nombre de points $\overline{E}_n = \dfrac{E_n-1}{q-1}$ de l'hypersurface *projective* est donc:

$$\overline{E}_n = \frac{q^n-1}{q-1} - \sum_{\substack{(a_1,\ldots,a_n)\in(\mathbf{Z}/d\,\mathbf{Z}-\{0\})^n \\ a_1+\ldots+a_n\neq 0}} \chi^{a_1+\ldots+a_n}(-1)\, J(\chi^{a_1},\ldots,\chi^{a_n}).$$

Lorsque $\chi_1\ldots\chi_n \neq 1$, on peut écrire $J(\chi_1,\ldots,\chi_n) = \dfrac{S(\chi_1)\ldots S(\chi_n)}{S(\chi_1\ldots\chi_n)}$, où $S(\chi) = \sum_a \chi(a)\lambda(a)$ est la somme de Gauss relative à un caractère additif λ fixé (*cf* [L], *p.* 4). Comme $|S(\chi)| = q^{1/2}$ pour $\chi \neq 1$, cela donne $|J(\chi_1,\ldots,\chi_n)| = q^{\frac{n-1}{2}}$ si χ_1, ..., χ_n, $\chi_1\ldots\chi_n \neq 1$; d'où l'estimation triviale:

$$|\overline{E}_n - \frac{q^n - 1}{q-1}| \leq q^{\frac{n-1}{2}} c_n,$$

où $c_n = Card\{(a_1,\ldots,a_n) \in (\mathbf{Z}/d\mathbf{Z}-\{0\})^n \mid a_1+\ldots+a_n \neq 0\}$.

On a visiblement $c_n = (d-1)^n - c_{n-1}$, d'où

$$c_n = (d-1)^n - (d-1)^{n-1} + \ldots + (-1)^{n-1}(d-1) = (1-\frac{1}{d})[(d-1)^n - (-1)^n].$$

On en conclut que $\overline{E}_n \neq 0$ dès que

$$\frac{q^n - 1}{q-1} > q^{\frac{n-1}{2}}(1-\frac{1}{d})[(d-1)^n - (-1)^n]$$

soit encore:

$$\frac{\sqrt{q}^n - \sqrt{q}^{-n}}{\sqrt{q} - \sqrt{q}^{-1}} > (1-\frac{1}{d})[(d-1)^n - (-1)^n].$$

Pour $n = 3$ et $d = 2^h$, on trouve le premier énoncé de 1). Finalement, on a $\frac{\sqrt{q}^n - \sqrt{q}^{-n}}{\sqrt{q} - \sqrt{q}^{-1}} > \sqrt{q}^{n-1}$ et $(1-2^{-h})[(2^h-1)^n - (-1)^n] < 2^{nh}$, d'où le deuxième énoncé.

Remarque 2.1. On notera que l'estimation de la prop. 1,1) ne donne aucun renseignement tant que $q \leq 2^{2h}$, tandis que le théorème de Chevalley montre que $\overline{E}_n \neq 0$ dès que $n \geq d$.

|| **Corollaire.** *Si n est une puissance de 2, la surface projective d'équation $x_0^n + x_1^n + x_2^n + x_3^n = 0$ a un point rationnel sur tout corps fini non premier.*

Démonstration. Cela résulte de *a*) et *b*) (début de la section) et de la prop. 1, 4) et 5).

Remarque 2.2. Nous baptiserons les inégalités de la prop. 1,1) *majorations de Jacobi-Weil.*

3. Une estimation modulaire

En reprenant la méthode de démonstration du théorème de Chevalley dans les corps finis ([CA], ch. 1), on obtient une formule pour la valeur modulo p du nombre de solutions de l'équation $x^{2^h} + y^{2^h} = -1$. On pourrait en principe l'utiliser pour tester si $s(p^3) = 2$. Toutefois, cette formule est une somme de