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

$(2^h-1)(2^{h-1}-1)$ termes, ce qui en pratique donne un temps de calcul bien trop long lorsque h devient grand: elle est donc peu intéressante en pratique, à moins qu'on n'arrive à la simplifier encore.

II **Proposition 2.** *Le nombre* N *de solutions dans* $\mathbf{F}_{q^2}$ *de l'équation* $x^{2^h}+y^{2^h} = -1$ *est congru modulo* p *à* $1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \left(\begin{smallmatrix} bi \\ bj \end{smallmatrix}\right)$, *où* $b = (q-1)/2^h$. *Si* $q = p^m$, *avec* m *impair, on a*

$$N \equiv 1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \left(\begin{smallmatrix} b_0 i \\ b_0 j \end{smallmatrix} \right)^m \pmod p,$$

où $b_0 = (p-1)/2^h$.

Démonstration. Soient $F(x,y) = x^{2^h}+y^{2^h}+1$ et $G(x,y) = 1-F(x,y)^{q-1}$. Alors $N \equiv \sum_{x,y \in \mathbf{F}_q} G(x,y)$ [CA], soit:

$$\begin{aligned} N &\equiv - \sum_{x,y \in \mathbf{F}_q} (x^{2^h}+y^{2^h}+1)^{q-1} \\ &\equiv - \sum_{x,y \in \mathbf{F}_q} \sum_{k=0}^{q-1} (-1)^k (x^{2^h}+y^{2^h})^k \\ &\equiv - \sum_{x,y \in \mathbf{F}_q} \sum_{k=0}^{q-1} (-1)^k \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) x^{2^h l} y^{2^h (k-l)} \\ &\equiv \sum_{k=0}^{q-1} (-1)^{k+1} \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) \sum_{x,y \in \mathbf{F}_q} x^{2^h l} y^{2^h (k-l)} \\ &\equiv \sum_{k=0}^{q-1} (-1)^{k+1} \sum_{l=0}^{k} \left(\begin{smallmatrix} k \\ l \end{smallmatrix} \right) \sum_{x \in \mathbf{F}_q} x^{2^h l} . \sum_{y \in \mathbf{F}_q} y^{2^h (k-l)} \pmod p. \end{aligned}$$

La somme $\sum_{x \in \mathbf{F}_q} x^{2^h l}$ (*resp.* $\sum_{y \in \mathbf{F}_q} y^{2^h (k-l)}$) est nulle, sauf si $2^h l \equiv 0 \pmod{q-1}$ et $2^h l > 0$ (*resp.* $2^h(k-l) \equiv 0 \pmod{q-1}$ et $2^h(k-l) > 0$), c'est-à-dire $l \equiv 0 \pmod b$ et $l > 0$ (*resp.* $k-l \equiv 0 \pmod b$ et $k-l > 0$); dans ce cas, elle vaut -1. Comme b est impair, on obtient donc:

$$N \equiv \sum_{i=2}^{2^h} (-1)^{bi+1} \sum_{j=1}^{i-1} \binom{bi}{bj} \equiv \sum_{i=2}^{2^h} (-1)^{i+1} \sum_{j=1}^{i-1} \binom{bi}{bj}.$$

Pour $i = 2^h$, on a $bi = q-1$, donc $\binom{bi}{bj} \equiv (-1)^{bj} \equiv (-1)^j \pmod p$, d'où

$$N \equiv 1 + \sum_{i=2}^{2^h-1} (-1)^{i+1} \sum_{j=1}^{i-1} \binom{bi}{bj} \pmod p.$$

Supposons maintenant $q = p^m$, avec m impair. Soient $l \le k < q$: écrivons $k = k_0 + k_1 p + \ldots + k_{m-1} p^{m-1}$ et $l = l_0 + l_1 p + \ldots + l_{m-1} p^{m-1}$, avec $0 \le k_i$, $l_i \le p-1$. On a alors:

$$\binom{k}{l} \equiv \prod_{i=0}^{m-1} \binom{k_i}{l_i} \pmod p;$$

cela résulte de l'identité $(X+Y)^k \equiv \prod_{i=0}^{m-1} (X^{p^i}+Y^{p^i})^{k_i} \pmod p$. On a $b = b_0(1+p+\ldots+p^{m-1})$, donc $ib = ib_0(1+p+\ldots+p^{m-1})$, avec $ib_0 \le p-1$ si $i \le 2^h$. Par conséquent, pour $0 \le j \le i \le 2^h$, on a:

$$\binom{bi}{bj} \equiv \binom{b_0 i}{b_0 j}^m \pmod p.$$

On en déduit l'énoncé.

|| **Corollaire.** *Supposons $q = p^m$, avec m impair. Si* $\sum_{i=2}^{2^h-1} (-1)^i \sum_{j=1}^{i-1} \binom{b_0 i}{b_0 j}^m \not\equiv 1 \pmod p$, *on a $s(q) = 2$.*

4. Cas des corps finis: résultats "expérimentaux"

Nous avons calculé la valeur de $s(p)$ pour tout $p < 10^9$, et celle de $s(p^3)$ pour tout $p < 104\,857\,601$. Ces calculs ont été réalisés sur un Macintosh II à l'aide d'un programme de Lightspeed Pascal et de la bibliothèque multiprécision de Dominique Bernardi. On retrouve ainsi comme cas particuliers les résultats de [PAR1], [PAR2], [PR] et [R] concernant les corps finis.

Les résultats complets, sous forme papier (129 pages) ou informatique, sont disponibles auprès des auteurs.

Phénomènes inexpliqués

Les données obtenues conduisent à un certain nombre d'observations *a priori* inattendues, auxquelles nous n'avons pas trouvé d'explication.

a) Taille de s

La propriété b) du §1, le théorème de Chevalley et la prop. 1,1) montrent qu'une majoration de s est donnée par

$$s \leq \min(l-1, 2^h),$$

et, si $p \geq 2^{2h}$,

$$(S1)\quad s \leq 1 + \left\lceil \frac{1}{\frac{\log(p)}{2h\log(2)} - 1} \right\rceil,$$

où l est le plus petit facteur premier impair de $p-1$, $h = h(p)$ et, pour tout réel a, $\lceil a \rceil$ désigne le plus petit entier $\geq a$.

En fait, hormis le cas des nombres premiers de Fermat (*cf* prop. 1,6)), les calculs montrent que la valeur réelle de s est nettement inférieure à cette majoration (voir table VIII). Pour tous les $p < 10^9$ on a $s \leq 12$ (Fermat exclus). De plus, les p ayant un grand s sont rares: jusqu'à 500 000 (resp. 10^9) il n'y a que 8 (resp. 61) nombres premiers p tels que $s(p) > 4$ (Fermat exclus).

b) Plus grand p pour lequel s > 2

D'après la prop. 1,1), la majoration de Jacobi-Weil affirme que l'on a $s(p) = 2$ dès que $p \geq 2^{4h(p)}$. Soient, pour tout $h \geq 2$, pour tout $s \geq 2$ et pour tout $t \geq 0$, $p_s(h)$ le plus grand nombre premier tel que $h(p) = h$ et $s(p) > s$ et $p_s(h,t)$ le plus grand nombre premier $\leq t$ tel que $h(p) = h$ et $s(p) > s$. Pour $h \leq 7$ on a $2^{4h} \leq 10^9$, donc $p_2(h,10^9) = p_2(h)$. La liste que nous obtenons est donc complète jusqu'à $h = 7$.

En fait, jusqu'à $h = 12$, le plus grand p trouvé est sensiblement inférieur à 10^9 (voir table I). Il est concevable qu'il existe (pour $8 \leq h \leq 12$) un $p > 10^9$ tel que $s(p) > 2$, mais cela impliquerait une forte irrégularité de la croissance des p (*cf* table VI). Les calculs montrent que, pour $4 \leq h \leq 7$, on a $\log(p_2(h))/h\log(2) \leq 2{,}72$ (pour $h = 3$, on a $\log(p_2(h))/h\log(2) = 3{,}19$).

Pour $h \geq 8$, on trouve encore $\log(p_2(h,10^9))/h\log(2) \leq 2{,}72$ (*cf* table I).

Il est curieux de constater que, pour $4 \leq h \leq 12$, les valeurs de $\log(p_2(h,10^9))/h\log(2)$ sont relativement proches, avec un écart-type de 2,7%; leur valeur moyenne est de 2,57, significativement inférieure à 4 (prédit par Jacobi-Weil).

b) Plus grand p pour lequel $s > 3$

La même étude dans ce cas conduit à des observations analogues (table II). Cette fois, la borne de Jacobi-Weil donne $p_3(h) \leq 2^{3h}$; on en déduit que $p_3(h,10^9) = p_3(h)$ pour $h \leq 9$. Pour $h \leq 9$, on trouve $\log(p_3(h))/h\log(2) \leq 1{,}72$; jusqu'à $h = 14$, on a vraisemblablement encore $p_3(h,10^9) = p_3(h)$. Pour ces valeurs de h, on trouve $\log(p_3(h,10^9))/h\log(2) \leq 1{,}74$. De nouveau, ce majorant est nettement inférieur à celui de Jacobi-Weil (3), et l'écart-type des valeurs de $\log(p_3(h,10^9))/h\log(2)$ est faible (1,62%).

c) Plus grand entier p pour lequel $s > 4$

Dans ce cas, les données sont plus partielles mais conduisent aux mêmes observations (table III). La valeur moyenne de $\log(p_4(h,10^9))/h\log(2)$, pour $h \leq 20$, est de 1,45 (les inégalités de Jacobi-Weil donneraient $8/3 = 2{,}66$).

d) Plus petit p pour lequel $s > 2$

Soit $P(h)$ le plus petit nombre premier p tel que $h(p) = h$ et $s(p) > 2$. Les calculs montrent que, pour $h \leq 25$, on a $(P(h)-1)/2^h \leq 749$; on a même $(P(h)-1)/2^h \leq 43$ pour $h \neq 7, 17$ (table IX). Il y a donc "assez tôt" des nombres premiers tels que $h > 2$. Quel est le comportement de $sup\ \{P(h) \mid h \leq H\}$ lorsque $H \to \infty$?

e) Plus petit p pour lequel $s = 3$

Soit $P'(h)$ le plus petit nombre premier p tel que $h(p) = h$ et $s(p) = 3$. Cette fois-ci, la croissance de $P'(h)$ en fonction de h est beaucoup plus rapide (pour $h \leq 17$); toutefois elle ne semble pas obéir à une règle bien déterminée (table X).

f) Valeur de $s(p^3)$

D'après la prop. 1,5), on a $s(p^3) \leq 3$. En fait, nos calculs montrent que,

jusqu'à $p \leq 101\,711\,873$, on a $s(p^3) = 2$. Plus précisément, il y a 21 nombres premiers $\leq 101\,711\,873$ pour lesquels les majorations de Jacobi-Weil autorisent que $s(p^3) = 3$; pour chacun de ces nombres premiers, on trouve en fait $s(p^3) = 2$. (Cette vérification demande un temps de calcul très long.) On a $2^{4h/3} < 10^9$ jusqu'à $h = 22$; on déduit de ceci et de nos calculs:

II **Proposition 3.** *Pour tout p tel que* $h(p) \leq 20$, *on a* $s(p^3) = 2$.

5. Questions ouvertes

5.1. Existe-t-il un nombre premier p tel que $s(p^3) = 3$? La question opposée est équivalente à la suivante (*cf* cor. à la prop. 1):

Si n est une puissance de 2, est-il vrai que la courbe projective d'équation $x^n+y^n+z^n = 0$ *a un point rationnel sur tout corps fini non premier?*

5.2. Les résultats observés en 3 a), b), c) correspondent-ils à un phénomène général? Plus spécifiquement, est-il vrai en général qu'en général, $c(s) := \inf\{\log(p_s(h))/h\log(2) \mid h > 1\}$ est sensiblement inférieur à $\frac{2s}{s-1}$ (donné par la prop. 1)? Nous pensons que oui, mais ne connaissons pas de motivation "théorique" pour ce phénomène hypothétique, et n'avons pas de conjecture sur la valeur de $c(s)$. Les résultats indiqués ci-dessus laisseraient penser que $c(2) < 2{,}8$, $c(3) < 1{,}8$, $c(4) < 1{,}5$. L'absence apparente de p tels que $s(p^3) = 3$ pourrait être liée à un tel phénomène (s'étendant aux corps finis non premiers).

On peut se demander s'il est même vrai que les majorations de Jacobi-Weil peuvent être améliorées dans le cas particulier des hypersurfaces considérées dans la prop. 1; nous n'avons pas fait de calculs dans ce sens. Une meilleure minoration de E_n (*cf* dém. de la prop. 1) n'est en tout cas pas nécessaire *a priori* pour justifier une meilleure majoration de $c(s)$.

On notera que le théorème de Chevalley apporte une information "arithmétique" que ne donnent pas les estimations "analytiques" à la Jacobi-Weil (*cf* remarque 2.2). Une meilleure majoration de $c(s)$ pourrait peut-être être obtenue à partir des congruences de la prop. 2, mais nous n'avons pas réussi à les exploiter dans ce sens.

5.3 (Revoy). Soit $\lambda(h) = \sup_{h(q)=h} s(q)$. D'après la prop. 1, 1), on a $\lambda(h) < +\infty$ pour tout h. Quel est le comportement de $\lambda(h)$ en fonction de h?

Les premières valeurs de $\lambda(h)$ sont données dans la table VIII (nombres premiers de Fermat exclus). S'il y a une infinité de nombres premiers de Fermat, on a $\lambda(h) = 2^h$ pour une infinité de h (prop. 1, 6)). Mais il est probable que $log\lambda(h) = o(h)$. En effet:

Proposition 4. *Soient* $N \geq 1$, $h \geq 2$ *et* p *un nombre premier tel que* $h(p) = h$. *Supposons que* $s(p) \geq 2^{h/N}$. *Alors:*

1) *Tout facteur premier de* $b = \frac{p-1}{2^h}$ *est* $> 2^{h/N}$.

2) *Soient* n_i *les exposants des facteurs premiers de* b. *Supposons* $\sum n_i > N$. *Alors on a* $2^{h/N}-1 \leq \frac{2}{\frac{\sum n_i}{N}-1}$ *et* $h \leq N\log_2(2N+1)$. *Pour* $N \leq 3$, *on a* $\sum n_i \leq N$.

Démonstration. 1) résulte immédiatement de la propriété (B). Supposons 2) faux. On a alors Supposons $\sum n_i > N$. Alors $log_2 p \leq 2\frac{2^{h/N}}{2^{h/N}-1} h$ (prop. 1, 1)). On a donc:

$$\frac{\sum n_i}{N} + 1 \leq 2\frac{2^{h/N}}{2^{h/N}-1}.$$

On en tire la première inégalité de 2). Pour obtenir la deuxième, on minore $\sum n_i$ par N+1. Finalement, supposons $N \leq 3$. Si $\sum n_i > N$ on a $h \leq N\log_2(2N+1) \leq 9$; pour ces valeurs de h on a $s(p) \leq 6$ (à l'exclusion de nombres de Fermat, *cf* table VIII), d'où $h \leq [3\log_2 6] = 7$. Avec cette nouvelle majoration de h, on a $s(p) \leq 5$ (*ibid.*), d'où $h \leq [3\log_2 5] = 6$. On vérifie directement que, pour $h \leq 6$, $(p-1)/2^h$ possède au plus 3 facteurs premiers, comptés avec multiplicité. (Pour $h \leq 6$, l'unique cas où $(p-1)/2^h$ possède 3 facteurs premiers est $p = 4001$, avec $h = 5$ et $s = 3$. Dans ce cas, on n'a donc pas $s(p) \geq 2^{h/N}$.)

Lorsque h est assez grand, le nombre $\frac{p-1}{2^h}$ doit avoir au plus N facteurs premiers (comptés avec multiplicité), tous grands en fonction de h. Il semble peu probable que, N étant fixé, il existe une infinité de h tels qu'un p vérifiant $h(p) = h$ ait cette propriété et vérifie de plus $s(p) \geq 2^{h/N}$.

Une réponse positive à la question 5.2 apporterait sans doute une amélioration importante des résultats de la prop. 4. Par exemple, s'il est vrai que $c(3) < 2$, $s(p) \geq 2^h$ implique $\sum n_i = 0$, *ie* que p est un nombre de Fermat. Si $c(4) < 1{,}5$, $s(p) \geq 2^{h/2}$ implique $\sum n_i \leq 1$. D'autre part, on peut voir que si $\sum n_i = N$, alors au moins un facteur premier de b est $\leq 2^{h/N}+2h\log(2)$. Par le théorème des nombres premiers, l'"espérance mathématique" d'un nombre premier dans l'intervalle $[2^{h/N}, 2^{h/N}+2h\log(2)]$ est 2 pour tout h; ceci laisse à penser que pour h assez grand, $\frac{p-1}{2^h}$ doit en fait avoir au plus N–1 facteurs premiers (comptés avec multiplicité).

5.4 (Revoy). Est-il vrai que $\sup_p s(p) = +\infty$? (De manière équivalente, est-il

vrai que $\lambda(h) \to \infty$, cf question 5.3.)

D'après la prop. 1, 6), cela serait vrai s'il y avait une infinité de nombres premiers de Fermat. On peut espérer que cela ne dépende pas de cette condition (puisqu'on a plutôt tendance à imaginer que les premiers de Fermat sont en nombre fini!). Plus généralement, on peut hasarder la

?? **Conjecture.** *Soient a et b deux entiers premiers entre eux; supposons que l'on n'aie $a \equiv 1 \pmod{l}$ pour aucun facteur premier impair l de b. Alors l'ensemble des $s(p)$, pour $p \equiv a \pmod{b}$, n'est pas borné.*

Dans l'énoncé, la condition sur b est mise pour prendre en considération la propriété (B) du §1. Cette conjecture implique que, si K est un corps quadratique imaginaire différent de $\mathbf{Q}(\sqrt{-3})$ ou un corps abélien de degré impair ne contenant aucune racine de l'unité d'ordre impair > 1, la suite $s_r(K)$ n'est pas bornée. (La condition "de degré impair" sur K est sans doute superflue.)

5.5. Quelle est la taille de $P(h)$ et de $P'(h)$ en général? (*cf* 3 d) et e)).

5.6. Soit $N(h)$ le nombre de p tels que $h(p) = h$ et que $s(p) > 2$; soit $N'(p)$ le nombre de ces p tels que $(p-1)/2^h$ soit premier. Les valeurs de $N(h)$ et $N'(h)$, pour h petit, apparaissent dans la table IV. Quelle est la taille de $N(h)$ et de $N'(h)$ en général, et comment varie la proportion $N'(h)/N(h)$? (L'étude de cette question a été suggérée par Etienne Fouvry.)

Références

[CA] J-P. Serre *Cours d'arithmétique*, P.U.F., Paris, 1970.

[L] S. Lang *Cyclotomic fields*, Graduate texts in Math. **59**, Springer, New York, 1978.

[P1] A. Pfister *Zur Darstellung von -1 als Summe von Quadraten in einem Körper*, J. London Math. Soc **40** (1965), 159-165.

[P2] A. Pfister *Multiplikative quadratische Formen*, Arch. Math. **16** (1965), 363-370.

[PAR1] J.C. Parnami, M.K. Agrawal, A.R. Rajwade, *On the fourth power Stufe of a field*, Rend. del Circ. Matem. di Palermo **30** (1981), 245-254.

[PAR2] J.C. Parnami, M.K. Agrawal, A.R. Rajwade, *On the fourth power Stufe of p-adic completions of algebraic number fields*, Rend. Sem. Mat. Univ. Politecn. Torino **44(1)** (1985), 141-153.

[PR] S. Pall, A.R. Rajwade *Power Stufe of Galois fields*, Bull. Soc. Math. Belg. **35** (1983), 123-130.

[R] P. Revoy *Niveaux supérieurs des corps et des anneaux*, C.R. Acad. Sci. Paris **307** (1988), 203-206.

Annexe: tables

Notations générales:

p: nombre premier
h: valuation dyadique de $p-1$
$s = s(p)$
l: plus petit facteur premier impair de $p-1$
$b = (p-1)/2^h$

I. Plus grandes valeurs de p telles que $s > 2$, pour $h \leq 12$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 4$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$	$\frac{1}{h}\log_2(10^9)$
5	**2**	**4**	**1**	**1,16**	
761	**3**	**3**	**5**	**3,19**	
977	**4**	**3**	**61**	**2,48**	
10 529	**5**	**3**	**7**	**2,67**	
83 009	**6**	**3**	**1297**	**2,72**	
397 697	**7**	**3**	**13**	**2,66**	
1 398 017	8	3	43	2,55	3,74
12 376 577	9	3	23	2,62	3,32
44 858 369	10	3	71	2,54	2,98
140 019 713	11	3	7	2,46	2,71
662 990 849	12	3	13	2,44	2,49

II. Plus grandes valeurs de p telles que $s > 3$, pour $h \leq 17$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 3$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$	$\frac{1}{h}\log_2(10^9)$
5	**2**	**4**	**1**	**1,16**	
41	**3**	**4**	**5**	**1,79**	
113	**4**	**4**	**7**	**1,70**	
353	**5**	**4**	**11**	**1,69**	
1 217	**6**	**4**	**19**	**1,71**	
4 481	**7**	**4**	**5**	**1,73**	
9 473	**8**	**4**	**37**	**1,65**	
45 569	**9**	**4**	**89**	**1,72**	
87 041	10	4	5	1,64	2,99
329 729	11	4	7	1,67	2,72
1 454 081	12	4	5	1,71	2,49
4 513 793	13	4	19	1,70	2,30
21 446 657	14	4	7	1,74	2,13
36 929 537	15	4	7	1,68	1,99
157 745 153	16	4	29	1,70	
410 386 433	17	4	31	1,68	

III. Plus grandes valeurs de p telles que $s > 4$, pour $h \leq 20$

Les valeurs en gras sont vraiment les plus grandes; les autres sont les plus grandes trouvées pour $p < 10^9$. (Majoration de Jacobi-Weil pour $\log(p)/h\log(2) : 8/3$.)

p	h	s	l	$\frac{1}{h}\log_2(p)$
449	**6**	**5**	**7**	**1,47**
3 329	**8**	**6**	**13**	**1,46**
13 313	**10**	**8**	**13**	**1,37**
59 393	**11**	**5**	**29**	**1,44**
176 129	12	5	43	1,45
1 073 153	13	5	131	1,54
2 277 377	14	5	139	1,51
4 882 433	15	5	149	1,48
8 716 289	16	5	7	1,44
31 326 209	17	5	239	1,46
64 749 569	18	5	13	1,44
103 284 737	19	5	197	1,40
409 993 217	20	5	17	1,43

IV. Nombre de p tels que $h(p) = h$ et $s(p) > 2$

On note $N(h,x)$ le nombre de $p \leq x$ tels que $h(p) = h$ et $s(p) > 2$, et $N(h) = N(h,\infty)$. Pour $h \leq 7$, on a $N(h,10^9) = N(h)$ par Jacobi-Weil; c'est probablement encore vrai jusqu'à $h = 12$ (cf. tableau I). Pour indiquer ceci, on a écrit $N(h)^*$ à la place de $N(h,10^9)$ pour $8 \leq h \leq 12$.

On note $N'(h,x)$ le nombre de $p \leq x$ tels que $h(p) = h$, $s(p) > 2$ et $(p-1)/2^h$ soit premier, et $N'(h) = N'(h,\infty)$. On a écrit $N'(h)^*$ à la place de $N'(h,10^9)$ pour $8 \leq h \leq 12$.

La fonction $\mathrm{Log}(N(h))/h$ semble croître lentement et irrégulièrement: c'est au moins ce qu'on constate pour $h \leq 12$, avec $\mathrm{Log}(N(h))/h \cong 0,53$.

$h = 2$	$N(h) = 2$	$N'(h) = 2$	$N'(h)/N(h) = 1$
$h = 3$	$N(h) = 5$	$N'(h) = 4$	$N'(h)/N(h) = 0,8$
$h = 4$	$N(h) = 5$	$N'(h) = 3$	$N'(h)/N(h) = 0,6$
$h = 5$	$N(h) = 13$	$N'(h) = 8$	$N'(h)/N(h) = 0,62$
$h = 6$	$N(h) = 23$	$N'(h) = 12$	$N'(h)/N(h) = 0,52$
$h = 7$	$N(h) = 39$	$N'(h) = 16$	$N'(h)/N(h) = 0,41$
$h = 8$	$N(h)^* = 69$	$N'(h)^* = 29$	$N'(h)^*/N(h)^* = 0,42$
$h = 9$	$N(h)^* = 110$	$N'(h)^* = 43$	$N'(h)^*/N(h)^* = 0,39$
$h = 10$	$N(h)^* = 217$	$N'(h)^* = 73$	$N'(h)^*/N(h)^* = 0,34$
$h = 11$	$N(h)^* = 359$	$N'(h)^* = 103$	$N'(h)^*/N(h)^* = 0,29$
$h = 12$	$N(h)^* = 708$	$N'(h)^* = 206$	$N'(h)^*/N(h)^* = 0,29$
$h = 13$	$N(h,10^9) = 1155$		
$h = 14$	$N(h,10^9) = 1163$		
$h = 15$	$N(h,10^9) = 709$		
$h = 16$	$N(h,10^9) = 371$		
$h = 17$	$N(h,10^9) = 171$		
$h = 18$	$N(h,10^9) = 88$		
$h = 19$	$N(h,10^9) = 50$		
$h = 20$	$N(h,10^9) = 28$		
$h = 21$	$N(h,10^9) = 14$		
$h = 22$	$N(h,10^9) = 6$		
$h = 23$	$N(h,10^9) = 4$		
$h = 24$	$N(h,10^9) = 0$		
$h = 25$	$N(h,10^9) = 1$		
$h = 26$	$N(h,10^9) = 1$		

V. Ensemble des $p < 10^9$ tels que $s > 2$ et $p < 2^{4h/3}$

Ces nombres premiers sont les seuls $< 10^9$ pour lesquels les majorations de Jacobi-Weil permettent que $s(p^3) > 2$.

p	h	s	l	$s(p^3)$
17	**4**	**16**	**1**	**2**
257	**8**	**256**	**1**	**2**
40 961	**13**	**4**	**5**	**2**
65 537	**16**	**65 536**	**1**	**2**
114 689	**14**	**6**	**7**	**2**
163 841	**15**	**4**	**5**	**2**
557 057	**15**	**9**	**17**	**2**
2 424 833	**16**	**6**	**37**	**2**
5 767 169	**19**	**10**	**11**	**2**
7 340 033	**20**	**6**	**7**	**2**
11 272 193	**18**	**7**	**43**	**2**
13 631 489	**20**	**12**	**13**	**2**
21 495 809	**19**	**8**	**41**	**2**
23 068 673	**21**	**10**	**11**	**2**
26 214 401	**20**	**4**	**5**	**2**
37 224 449	**19**	**6**	**71**	**2**
40 370 177	**19**	**6**	**7**	**2**
70 254 593	**20**	**6**	**67**	**2**
101 711 873	**20**	**6**	**97**	**2**
104 857 601	22	4	5	
111 149 057	21	7	53	
136 314 881	21	4	5	
155 189 249	22	10	37	
167 772 161	25	4	5	
186 646 529	21	7	89	
199 229 441	21	4	5	
211 812 353	21	6	101	
230 686 721	22	4	5	
249 561 089	21	6	7	
469 762 049	26	6	7	
595 591 169	23	7	71	
645 922 817	23	6	7	
897 581 057	23	7	107	
998 244 353	23	6	7	

VI. Valeurs de s pour $h(p) = 6$

L'entier s_1 est défini par le membre de droite de l'inégalité (S1) du §3, a) (pour $p > 2^{2h} = 4096$).

p	h	s	s_1	l
449	6	5		7
1 217	6	4		19
2 753	6	3		43
3 137	6	3		7
4 289	6	3	182	67
4 673	6	3	65	73
5 441	6	3	31	5
6 977	6	3	17	109
9 281	6	3	12	5
10 433	6	3	10	163
11 969	6	3	9	11
13 121	6	3	9	5
15 809	6	3	8	13
25 409	6	3	6	397
25 793	6	3	6	13
26 177	6	3	6	409
26 561	6	3	6	5
29 633	6	3	6	463
33 857	6	3	5	23
52 289	6	3	5	19
53 441	6	3	5	5
64 577	6	3	5	1009
83 009	6	3	4	1297

VII. Les 12 derniers $p < 10^9$ tels que $h(p) = 12$ et $s(p) > 2$

p	h	s	s_1	l
386 019 329	12	3	7	73
390 270 977	12	3	7	151
398 233 601	12	3	7	5
416 223 233	12	3	7	307
434 040 833	12	3	7	105 967
459 182 081	12	3	7	5
491 696 129	12	3	6	7
502 067 201	12	3	6	5
524 185 601	12	3	6	5
561 246 209	12	3	6	263
588 648 449	12	3	6	137
662 990 849	12	3	6	13

VIII. Valeurs maximales de s en fonction de h trouvées pour $p < 10^9$ (nombres de Fermat exclus)

$W = 2^{sh/(s-1)}$; tant que $W < 10^9$, c'est effectivement la valeur maximale grâce aux majorations de Jacobi-Weil.

h	s	p	W
2	4	5	40
3	4	41	256
4	4	113	1 625
5	4	353	10 321
6	5	449	32 768
7	4	641	416 127
8	6	3 329	602 248
9	4	11 777	16 777 216
10	8	13 313	7 597 760
11	5	59 393	189 812 531
12	6	151 553	467 373 274
13	7	188 417	1 352 829 926
14	6	114 689	13 019 906 170
15	9	557 057	10 822 639 410
16	6	2 424 833	
17	5	19 529 729	
18	7	11 272 193	
19	10	5 767 169	
20	12	13 631 489	
21	10	23 068 673	
22	10	155 189 249	
23	7	595 591 169	
24			
25	4	167 772 161	
26	6	469 762 049	

IX. Plus petite valeur de p pour laquelle $s > 2$

p	h	s	l	b
41	3	4	5	5
17	4	16	1	1
113	4	4	7	7
353	5	4	11	11
449	6	5	7	7
95 873	7	3	7	$749 = 7 \cdot 107$
257	8	256	1	1
3 329	8	6	13	13
11 777	9	4	23	23
13 313	10	8	13	13
59 393	11	5	29	29
151 553	12	6	37	37
40 961	13	4	5	5
114 689	14	6	7	7
163 841	15	4	5	5
65 537	16	65 536	1	1
2 424 833	16	6	37	37
19 529 729	17	5	149	149
11 272 193	18	7	43	43
5 767 169	19	10	11	11
7 340 033	20	6	7	7
23 068 673	21	10	11	11
104 857 601	22	4	5	$25 = 5^2$
595 591 169	23	7	71	71
167 772 161	25	4	5	5
469 762 049	26	6	7	7

X. Plus petite valeur de p pour laquelle $s = 3$

p	h	s	l
89	3	3	11
401	4	3	5
929	5	3	29
4 289	6	3	67
95 873	7	3	7
14 081	8	3	5
17 921	9	3	5
136 193	10	3	7
366 593	11	3	179
643 073	12	3	157
3 383 297	13	3	7
3 260 417	14	3	199
6 258 689	15	3	191
20 512 769	16	3	313
67 502 081	17	3	5

Pour $h \geq 18$, on ne trouve aucun $p < 10^9$ pour lequel $s = 3$.

Yvette AMICE et Bruno KAHN
Université de Paris 7
UFR de Mathématiques
5ème étage, couloir 45–55
2, Place Jussieu
75251 PARIS Cedex 05
FRANCE
adresses électroniques :
amice@mathp7.jussieu.fr
kahn@mathp7.jussieu.fr