Canad. Math. Bull. Vol. **38** (3), 1995 pp. 304–307

POLYNÔMES ANISOTROPES MODULO p^2

EL MOSTAFA HANINE

RÉSUMÉ. Nous proposons de construire des polynômes à coefficients p-adiques, de degré D, sans terme constant, ayant plus que $2D+1$ variables. Ces polynômes n'ont dans Z_p que le zéro trivial modulo p^2. Le but que nous cherchons à atteindre, à partir des polynômes ainsi construit, est de minorer les valeurs de p pour lesquelles l'équation $F(x_1,\ldots,x_{2D+1}) \equiv 0 \pmod{p^2}$ admet une solution primitive, F est un élément de $Z_p[X_1,\ldots,X_{2D+1}]$ de degré D sans term constant.

1. **Introduction.** Nous nous intéressons dans cette étude aux équations diophantiennes modulo p^2.

J. Ax et S. Kochen ont démontré que pour tout entier $d \geq 1$, il existe un plus petit entier $p(d)$, tel que si p est un nombre premier supérieur ou égal à $p(d)$, tout polynôme sans term constant $F \in \mathbf{Q}_p[X_1,\ldots,X_n]$ de degré d, où $n > d^2$, a un zéro non nul dans $\mathbf{Q}_p^n$ ([2] théorème de la page 445).

Dans [1] nous avons démontré un résultat analogue à celui de J. Ax et S. Kochen, qui s'énonce comme suit : Pour tout entier $d \geq 1$, il existe un plus petit nombre premier $p(d)$ tel que si $p \geq p(d)$, pour tout F élément de $\mathbf{Z}_p[X_1,\ldots,X_{2d+1}]$ de degré d sans terme constant, l'équation $F(x_1,\ldots,x_{2d+1}) \equiv 0 \pmod{p^2}$ admet une solution primitive.

Nous avons aussi démontré dans le même article, que $p(2) = 2, p(3) = 3$ et que pour tout $d \geq 4$ on a $p(d) > 2$.

Dans ce papier, nous proposons de construire des polynômes à coefficients p-adiques, de degré D, sans terme constant, ayant plus que $2D+1$ variables et n'ayant dans $\mathbf{Z}_p$ que le zéro banal modulo p^2. Ceci nous permettra de démontrer que :

i) pour tout entier $D \geq 6$ et différent de 8, $p(D) > 3$

ii) pour tout entier $D \geq \frac{2p^2+p}{p-1}$, $p(D) > p$.

2. **Définitions et propriétés.**

DÉFINITION. Soient A un anneau intègre et $f \in A[X_1,\ldots,X_n]$ un polynôme sans terme constant. On dit que f est anisotrope si pour tout $(x_1,\ldots,x_n) \in A^n$, la relation $f(x_1,\ldots,x_n) = 0$ entraîne : $x_1 = x_2 = \cdots = x_n = 0$. Dans le cas où $A = \mathbf{Z}_p$, on dit que f est anisotrope modulo p^a, où a est un entier ≥ 1, si pour tout $(x_1,\ldots,x_n) \in Z_p^n$, la relation $f(x_1,\ldots,x_n) \equiv 0 \pmod{p^a}$ entraîne $x_1 \equiv x_2 \equiv \cdots \equiv x_n \equiv 0 \pmod{p}$.

Dans ce qui suit on notera n_d une forme norme de $\mathbf{Z}_p[X_1,\ldots,X_d]$, de degré d, et anisotrope modulo p ; une telle form s'obtient en relevant dans $\mathbf{Z}_p$, une forme norme de l'extension de degré d de $\mathbf{F}_p$.

Reçu par les éditeurs le 23 avril 1993; réviseé 26 janvier, 1994.
Classification (AMS) par sujet : 11D88.
© Société mathématique du Canada 1995.

https://doi.org/10.4153/CMB-1995-044-2 Published online by Cambridge University Press

DÉFINITION. On dit que $(x_1,\dots,x_n) \in Z_p^n$ est *primitif*, si l'un des x_i est non divisible par p.

PROPOSITION 2.1. *Soit $d \in \mathbf{N}^*$, et soit p un nombre premier, pour tout $(x_1,\dots,x_d)$ élément de Z_p^d, primitif,* $\big(n_d(x_1,\dots,x_d)\big)^{(p^2-p)} \equiv 1 \pmod{p^2}$.

DÉMONSTRATION. Pour tout $(x_1,\dots,x_d)$ élément de Z_p^d primitif $n_d(x_1,\dots,x_d) \not\equiv 0 \pmod p$ ce qui implique $\big(n_d(x_1,\dots,x_d)\big)^{(p^2-p)} \equiv 1 \pmod{p^2}$.

PROPOSITION 2.2. *Soit p un entier naturel premier, pour tout $(x,y) \in \mathbf{Z}_P^2$,*

$$x^p y^p \equiv x^p y + xy^p - xy \pmod{p^2}.$$

DÉMONSTRATION. $x^p \equiv x \pmod p$ *et* $y^p \equiv y \pmod p$ *ce qui entraîne* $x^p - x \equiv 0 \pmod p$ *et* $y^p - y \equiv 0 \pmod p$ *d'où :* $(x^p - x)(y^p - y) \equiv 0 \pmod{p^2}$.

PROPOSITION 2.3. *Soit p un entier premier supérieur à 2 et soit d un entier ≥ 1, on a pour tout $x \in \mathbf{Z}$:*

i) Pour tout entier $s \geq 1$, $x^{d(p^2-p)} \equiv x^{s(p^2-p)} \pmod{p^2}$.

ii) Pour tout entier s, $x^{d(p^2-p)} \equiv x^{s(p^2-p)}(2x^{p+1} - x^2)^{(p-1)/2} \pmod{p^2}$.

iii) Pour tout entier $t \geq 1$, il exist $v_t \in Z[X]$, de degré $\leq 2p-1$ et sans terme constant vérifiant : $x^t \equiv v_t(x) \pmod{p^2}$.

DÉMONSTRATION. Pour démontrer i), on distingue deux cas.

1ER CAS. Si p ne divise pas x, on a $x^{p^2-p} \equiv 1 \pmod{p^2}$. Donc pour tout entier $s \geq 1$:

$$x^{d(p^2-p)} \equiv x^{s(p^2-p)} \pmod{p^2}.$$

2ÈME CAS. Si p divise x, la propriété est triviale.

La propriété i) permet d'écrire :

$$\begin{aligned} x^{d(p^2-p)} &\equiv x^{(s+1)(p^2-p)} \pmod{p^2} \\ &\equiv x^{s(p^2-p)}(x^{2p})^{(p-1)/2} \pmod{p^2}. \end{aligned}$$

D'après la proposition 2.2, on a $x^{2p} \equiv 2x^{p+1} - x^2 \pmod{p^2}$, d'où ii). La démonstration de iii) se déduit par récurrence à partir de la proposition 2.2.

CONSÉQUENCE 2.4. Soient $k \in \mathbf{N}^*$ et $(\beta_1,\dots,\beta_k) \in N^k - \{(0,\dots,0)\}$, alors il existe $u_k \in \mathbf{Z}_p[X_1,\dots,X_k]$ de degré $\leq (2p-1)+(k-1)(p-1)$, sans terme constant, tel que : pour tout $(x_1,\dots,x_k) \in Z^k$, $x_1^{\beta_1}\cdots x_k^{\beta_k} \equiv u_k(x_1,\dots,x_k) \pmod{p^2}$.

DÉMONSTRATION. Immédiate d'après les propositions 2.2 et 2.3.

https://doi.org/10.4153/CMB-1995-044-2 Published online by Cambridge University Press

PROPOSITION 2.5. *Pour tout entier d supérieur ou égal à 1 et pour tout nombre premier p, il existe des polynômes $f \in \mathbf{Z}_p[X_1,\dots,X_d]$, sans terme constant de degré D supérieur ou égal à $(2p-1)+(d-1)(p-1)$, vérifiant : pour tout $(x_1,\dots,x_d) \in \mathbf{Z}_p^d$, $\big(n_d(x_1,\dots,x_d)\big)^{(p^2-p)} \equiv f(x_1,\dots,x_d) \pmod{p^2}$.*

DÉMONSTRATION. En vertu de la proposition 2.3 et la conséquence 2.4, il existe $f_1 \in \mathbf{Z}_p[X_1,\dots,X_d]$, de degré inférieur ou égal à $(2p-1)+(d-1)(p-1)$ et sans terme constant, tel que : pour tout $(x_1,\dots,x_d) \in Z_p^d$, $\big(n_d(x_1,\dots,x_d)\big)^{(p^2-p)} \equiv f_1(x_1,\dots,x_d) \pmod{p^2}$.

Si degré $f_1 = D$ on pose $f = f_1$. Sinon, on considère $f = p^2X_1^D + f_1$. f vérifie alors la proposition.

3. Construction des polynômes anisotropes modulo p^2.

LEMME 3.1. *Le polynôme*

$$F = f(X_1,\dots,X_d) + f(X_{d+1},\dots,X_{2d}) + \cdots + f(X_{d(p^2-2)+1},\dots,X_{d(p^2-1)})$$

(où f est le polynôme de la proposition 2.3) est anisotrope modulo p^2.

DÉMONSTRATION. Soit $(x_1,\dots,x_{d(p^2-1)})$ un élément de $\mathbf{Z}_p^{d(p^2-1)}$, avec l'une des composantes non divisible par p, on peut supposer que c'est x_1 d'où

$$\big(n_d(x_1,\dots,x_d)\big)^{(p^2-p)} \equiv f_1(x_1,\dots,x_d) \equiv 1 \pmod{p^2}.$$

Ceci entraîne que $F(x_1,\dots,x_{d(p^2-1)}) \equiv n \pmod{p^2}$ avec $1 \le n \le p^2-1$, on en déduit que F est anisotrope modulo p^2.

THÉORÈME 3.1. *Soit p est un nombre premier, et soit D un entier > 1, alors si $D \ge \frac{2p^2+p}{p-1}$ on a $p(D) > p$.*

DÉMONSTRATION. D'après le lemme précédent, il suffit de prouver l'existence d'un entier d vérifiant :

$$\begin{aligned} 2D+1 &\le d(p^2-1) \\ p+d(p-1) &\le D \end{aligned} \tag{1}$$

Le système (1) est équivalent à :

$$\frac{2D+1}{p^2-1} \le d \le \frac{D-p}{p-1}.$$

Une condition nécessaire pour l'existence d'un entier d vérifiant (1) est que : $\frac{D-p}{p-1} - \frac{2D+1}{p^2-1} \ge 1$, c'est à dire $D \ge \frac{2p^2+p}{p-1}$ ce qui démontre le théorème.

Dans le cas $p = 3$, le théorème précédent montre que $p(D) > 3$ pour tous les entiers $D \ge 11$. En remarquant que les couples (7,2), (9,3) et (10,3) sont solutions du système (1), on montre que $p(7)$, $p(9)$ et $p(10)$ sont aussi supérieurs strictement à 3.

https://doi.org/10.4153/CMB-1995-044-2 Published online by Cambridge University Press

Dans ce qui suit on va montrer qu'on a $p(6) > 3$. Pour cela considérons le polynôme :

$$n_2(X, Y) = X^2 + Y^2, \quad \text{qui est anisotrope modulo 3.}$$

On a :

$$\big(n_2(X, Y)\big)^6 = X^{12} + 6X^{10}Y^2 + 15X^8Y^4 + 20X^6Y^6 + 15X^4Y^8 + 6X^2Y^{10} + Y^{12}.$$

D'aprés les propositions 2.2 et 2.3, on a pour tout $(x, y) \in Z^2$,

$$\begin{aligned}
x^{12} &\equiv x^6 \pmod 9\\
y^{12} &\equiv y^6 \pmod 9\\
x^{10}y^2 &\equiv x^4y^2 \pmod 9\\
x^8y^4 &\equiv x^2y^4 \pmod 9\\
x^6y^6 &\equiv 2x^4y^2 + 2x^2y^4 - 3x^2y^2 \pmod 9\\
x^2y^{10} &\equiv x^2y^4 \pmod 9\\
x^4y^8 &\equiv x^4y^2 \pmod 9.
\end{aligned}$$

D'après ce système on peut déduire que :

$$\begin{aligned}
&x^{12}+6x^{10}y^2 + 15x^8y^4 + 20x^6y^6 + 15x^4y^8 + 6x^2y^{10} + y^{12}\\
&\quad \equiv x^6 6x^4y^2 + 15x^2y^4 + 20(2x^4y^2 + 2x^2y^4 - 3x^2y^2) + 15x^4y^2 + 6x^2y^4 + y^6 \pmod 9.
\end{aligned}$$

Après regroupement des différents termes du second membre, on obtient : $x^6+61x^4y^2+61x^2y^4 - 60x^2y^2 + y^6$.

Considérons maintenant le polynôme :

$$f(X, Y) = X^6 + 61X^4Y^2 + 61X^2Y^4 - 60X^2Y^2 + Y^6,$$

on a pour tout $(x, y) \in \mathbf{Z}^2, f(x, y) \equiv \big(n_2(x, y)\big)^6 \pmod 9$.

Il en résulte alors que : $F(X_1, \ldots, X_{16}) = f(X_1, X_2) + f(X_3, X_4) + \cdots + f(X_{15}, X_{16})$ est aussi de degré 6 et anisotrope modulo 9. Finalement on en déduit que $p(6)$ est strictement supérieur à 3.

RÉFÉRENCES

1. Hanine El Mostafa, *Equations Diophantiennes p-adiques modulo p^2*, Colloq. Math. (2) **LXIV**(1993), 1139–1144.

2. J. Ax and S. Kochen, *Diophantine problems over local fields, III*, Ann. of Math. (3) **83**(1966), 437–456.

Université Paul Sabatier
Laboratoire d'Algèbre
118 Route de Narbonne
31062 Toulouse Cedex
France

https://doi.org/10.4153/CMB-1995-044-2 Published online by Cambridge University Press