COLLOQUIUM MATHEMATICUM
VOL. LXIV 1993 FASC. 2

ÉQUATIONS DIOPHANTIENNES MODULO p^2

BY

EL MOSTAFA HANINE (TOULOUSE)

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 terme constant $F \in \mathbb{Q}_p[X_1, \ldots, X_n]$ de degré d, où $n > d^2$, a un zéro non nul dans $\mathbb{Q}_p^n$ ([2], théorème de la page 445).

Nous nous proposons ici de démontrer un résultat analogue à celui de J. Ax et S. Kochen, qui s'énonce comme suit :

Pour tout entier $d \geq 2$, il existe un plus petit entier $p(d)$ tel que si $p \geq p(d)$, avec p un nombre premier, pour tout polynôme $F \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}]$ de degré d et sans terme constant, l'équation $F(X_1, \ldots, X_{2d+1}) \equiv 0 \pmod{p^2}$ admet une solution primitive.

Nous démontrons aussi que $p(2) = 2$, $p(3) = 3$, et pour tout $d \geq 4$, nous construisons des polynômes de degré d sans terme constant, dépendant de plus de $2d+1$ variables et anisotropes modulo 4 (c.à.d. $p(d) > 2$ pour tout $d \geq 4$).

Pour d multiple de $p^2 - p$ on construit des polynômes homogènes de degré d, dépendant de plus de $2d+1$ variables et anisotropes modulo p^2 (c.à.d. si d est multiple de $p^2 - p$, on a $p(d) > p$).

1. Théorème analogue au théorème de J. Ax et S. Kochen

THÉORÈME. *Soit d un entier supérieur ou égal à 2. Il existe un nombre $p(d)$ tel que si p est un nombre premier supérieur ou égal à $p(d)$, et $F \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}]$ est un polynôme sans terme constant, de degré d, il existe alors un élément $X \in \mathbb{Z}_p^{2d+1}$ dont l'une des composantes au moins n'est pas divisible par p et tel que $F(X) \equiv 0 \pmod{p^2}$.*

P r e u v e. Soit $A_p = \mathbb{F}_p[[T]]$ l'anneau des séries formelles à coefficients dans $\mathbb{F}_p$, où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Soit $F \in A_p[X_1, \ldots, X_{2d+1}]$ un polynôme de degré d sans terme constant. On peut écrire F sous la forme

$$F(X_1, \ldots, X_{2d+1}) = f_1(X_1, \ldots, X_{2d+1}) + f_2(X_1, \ldots, X_{2d+1})T + \ldots$$

où $f_i \in \mathbb{F}_p[X_1, \ldots, X_{2d+1}]$ et $\deg f_i \leq d$; d'où

$$F(X_1, \ldots, X_{2d+1}) \equiv f_1(X_1, \ldots, X_{2d+1}) + f_2(X_1, \ldots, X_{2d+1})T \pmod{T^2}.$$

Considérons maintenant le système

$$f_1(X_1, \ldots, X_{2d+1}) = 0\,, \quad f_2(X_1, \ldots, X_{2d+1}) = 0\,.$$

On a $\deg f_1 + \deg f_2 \leq 2d$. D'après le théorème de Chevalley–Warning, il existe alors $(x_1, \ldots, x_{2d+1})$ élément de $\mathbb{F}_p^{2d+1} - \{(0, \ldots, 0)\}$ tel que

$$f_1(x_1, \ldots, x_{2d+1}) = 0\,, \quad f_2(x_1, \ldots, x_{2d+1}) = 0\,,$$

ce qui nous donne $F(x_1, \ldots, x_{2d+1}) \equiv 0 \pmod{T^2}$.

D'autre part, dans la théorie des corps valués (K, v) à valeurs dans un $\mathbb{Z}$-groupe, pour un entier $d \geq 1$ fixé, la propriété : "pour tout F de $K[X_1, \ldots, X_{2d+1}]$ de degré d sans terme constant et à coefficients entiers, il existe $x \in K^{2d+1}$ à coordonnées entières, l'une des coordonnées de x étant de valuation nulle, tel qu'on ait $v(F(x)) \geq 2$", est une propriété élémentaire qu'on notera $\Gamma(d)$. On a le principe général suivant :

Pour toute propriété élémentaire Δ, il existe un nombre premier $p(\Delta)$ tel que si p est un nombre premier $\geq p(\Delta)$, Δ est vraie dans $\mathbb{Z}_p$ si et seulement si Δ est vraie dans l'anneau des séries formelles à une indéterminée sur le corps fini $\mathbb{F}_p$ (Théorème 6, page 629 de [1]).

La démonstration de ce principe général relève de notions de logique mathématique. On trouvera ces démonstrations ainsi que la définition de la "propriété élémentaire" dans [2]. Dans ce qui suit, on prendra pour $p(d)$ le plus petit des $p(\Gamma(d))$.

2. Les polynômes singuliers sans terme constant, sur un corps fini

Définition. Soient K un corps et f un élément de $K[X_1, \ldots, X_n]$ non nul et sans terme constant; on dit que f est *singulier* si pour tout $x = (x_1, \ldots, x_n) \in K^n - \{(0, \ldots, 0)\}$ tel que $f(x) = 0$, on a $(\partial f/\partial X_i)(x) = 0$ pour tout $1 \leq i \leq n$.

2.1. Proposition. *Soient K un corps fini et d un entier supérieur ou égal à 2. Soit f un élément de $K[X_1, \ldots, X_n]$ de degré d, non nul et sans terme constant avec $n \geq 2d$. Alors si f est singulier, la composante homogène de degré 1 est nulle.*

Preuve. Ecrivons f sous la forme $f = f_d + f_{d-1} + \ldots + f_1$, où les f_j sont des polynômes homogènes de degré j. Le polynôme f_1 étant de degré 1, nous pouvons l'écrire sous la forme $f_1(X) = a_1X_1 + \ldots + a_nX_n$.

D'après le théorème de Chevalley–Warning, le système

$$f(X) = 0, \qquad \frac{\partial(f_d + f_{d-1} + \ldots + f_2)}{\partial X_i}(X) = 0$$

admet une solution non nulle $x = (x_1, \ldots, x_n)$ dans K^n. Comme f est singulier, nous avons

$$\frac{\partial f}{\partial X_i}(x) = \frac{\partial}{\partial X_i}(f_d + \ldots + f_2)(x) + \frac{\partial f_1}{\partial X_i}(x) = 0 + a_i = 0$$

pour tout i; nous déduisons que $f_1 = 0$.

3. Les polynômes de degré 2 et sans terme constant

3.1. Proposition. *La fonction polynomiale d'une forme quadratique non nulle à coefficients dans un anneau commutatif unitaire est non nulle.*

P r e u v e. Soit A un anneau commutatif unitaire et soit q une forme quadratique non nulle; alors il existe $(x_1, \ldots, x_n)$ élément de A_n tel que $q(x_1, \ldots, x_n) \neq 0$. Sinon, en écrivant q sous la forme

$$q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq n} a_{ii} X_i^2 + \sum_{1 \leq i < j \leq n} a_{ij} X_i X_j$$

nous avons

$$q(0, \ldots, 0, 1, 0, \ldots, 0) = a_{ii} = 0 \quad \text{quel que soit } 1 \leq i \leq n \text{ et}$$
$$q(0, \ldots, 0, 1, 0, \ldots, 0, 1, 0, \ldots, 0) = a_{ii} + a_{jj} + a_{ij} = 0,$$
$$\text{si 1 est la } i^{\text{ème}} \text{ et la } j^{\text{ième}} \text{ coordonnée.}$$

Nous en déduisons que $q = 0$.

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 $x_1 = \ldots = x_n = 0$. Dans le cas où $A = \mathbb{Z}_p$, on dit que f est *anisotrope modulo* p^a, où a est entier ≥ 1, si pour tout $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$, la relation $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^a}$ entraîne

$$x_1 \equiv \ldots \equiv x_n \equiv 0 \pmod{p}.$$

3.2. Lemme. *Soit K un corps commutatif, et soit $f \in K[X_1, \ldots, X_n]$ un polynôme singulier non nul, de degré 2 et sans terme constant; alors f est anisotrope, ou bien il existe une forme quadratique anisotrope $g \in K[X_1, \ldots, X_k]$ telle que $f = g(L_1, \ldots, L_k)$, où $k < n$ et les L_i sont des formes de degré 1.*

P r e u v e. Si f n'est pas anisotrope, on considère $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ tel que $f(a_1, \ldots, a_n) = 0$. Il existe une transformation linéaire inversible et

homogène des variables $X_i = \sum_{1\le j\le n} l_{ij}Y_j$ telle que $(0,\dots,0,1)$ soit l'image de $(a_1,\dots,a_n)$.

En posant $f(X_1,\dots,X_n) = h(Y_1,\dots,Y_n)$ on a $h(0,\dots,0,1) = 0$ on peut écrire $h(Y_1,\dots,Y_n)$ sous la forme

$$h(Y_1,\dots,Y_n) = a_nY_n^2 + Y_n(a_1Y_1 + \dots + a_{n-1}Y_{n-1}) + b_1Y_1 + \dots + b_nY_n + g(Y_1,\dots,Y_{n-1})\,,$$

où g est un polynôme homogène de degré 2. On a

$$h(0,\dots,0,1) = a_n + b_n = 0\,. \tag{1}$$

Comme f est singulier, alors il en est de même pour h, d'où

$$\frac{\partial h}{\partial Y_n}(0,\dots,0,1) = 2a_n + b_n = 0\,. \tag{2}$$

D'après (1) et (2) on a $a_n = b_n = 0$, ce qui nous donne

$$h(Y_1,\dots,Y_n) = Y_n(a_1Y_1 + \dots + a_{n-1}Y_{n-1}) + b_1Y_1 + \dots + b_{n-1}Y_{n-1} + g(Y_1,\dots,Y_{n-1})\,.$$

L'expression $a_1Y_1+\dots+a_{n-1}Y_{n-1}$ est nulle : sinon il existe $(c_1,\dots,c_n) \in K^n$ tel que $a_1c_1 + \dots + a_{n-1}c_{n-1} \neq 0$ et $h(c_1,\dots,c_n) = 0$. Dans ce cas $(c_1,\dots,c_n)$ est un zéro non singulier de h, ce qui est impossible.

D'autre part, pout tout $1 \le i \le n-1$,

$$\frac{\partial h}{\partial Y_i}(0,\dots,0,1) = b_i = 0\,,$$

car $h(0,\dots,0,1) = 0$, d'où $h(Y_1,\dots,Y_n) = g(Y_1,\dots,Y_{n-1})$.

Dans le cas où g n'est pas anisotrope, on répètera le même processus sur g. Au bout d'un nombre fini de fois, on obtiendra f sous la forme $f = g(L_1,\dots,L_k)$, avec g forme quadratique anisotrope et $L_1,\dots,L_k$ des formes linéaires.

Définition. On dit que $(x_1,\dots,x_n) \in \mathbb{Z}_p^n$ est *primitif* si l'un des x_i n'est pas divisible par p.

3.3. Proposition. *Pour tout $f \in \mathbb{Z}_p[X_1,\dots,X_5]$ de degré 2 et sans terme constant, il existe $(x_1,\dots,x_5) \in \mathbb{Z}_p^5$ primitif tel que $f(x_1,\dots,x_5) \equiv 0 \pmod{p^2}$.*

Preuve. 1er cas : Si $\bar{f}$ est nul (où $\bar{f}$ est le polynôme de $\mathbb{F}_p[X_1,\dots,X_5]$ obtenu en réduisant les coefficients de f modulo p), alors il existe h élément de $\mathbb{Z}_p[X_1,\dots,X_5]$ tel que $f = ph$. D'après le théorème de Chevalley–Warning, $h \equiv 0 \pmod{p}$ admet une solution primitive $(x_1,\dots,x_5)$ et cette solution vérifie $f(x_1,\dots,x_5) \equiv 0 \pmod{p^2}$.

$2^{\text{ème}}$ c a s : Si $\bar{f}$ est non nul et non singulier, alors il existe $(x_1,\dots,x_5)\in\mathbb{Z}_p^5$ primitif et $1\le i_0\le 5$ tels que

$$f(x_1,\dots,x_5)\equiv 0 \pmod p \quad\text{et}\quad \frac{\partial f}{\partial X_{i_0}}(x_1,\dots,x_5)\not\equiv 0 \pmod p\,.$$

D'après le lemme de Hensel il existe $(y_1,\dots,y_5)\in\mathbb{Z}_p^5$ primitif tel que $f(y_1,\dots,y_5)=0$, ce qui implique que $f(y_1,\dots,y_5)\equiv 0 \pmod{p^2}$.

$3^{\text{ème}}$ c a s : Si $\bar{f}$ est non nul et singulier, d'après le lemme précédent, $\bar{f}$ peut s'écrire sous la forme $\bar{f}=g(L_1,\dots,L_k)$, où g est anisotrope et les L_i sont des formes linéaires. D'après la proposition 2.1, $\bar{f}$ est homogène, donc g l'est aussi. Le théorème de Chevalley–Warning permet d'affirmer que g dépendra au plus de deux variables, dont $\bar{f}=g(L_1,L_2)$, avec L_1 et L_2 des formes linéaires qui peuvent être égales.

Soit $g'\in\mathbb{Z}_p[X_1,X_2]$ de degré 2 tel que $\overline{g'}=g$. Soient L_1', L_2' des formes linéaires de $\mathbb{Z}_p[X_1,\dots,X_5]$ telles que $\overline{L_1'}=L_1$ et $\overline{L_2'}=L_2$, et soit $h\in\mathbb{Z}_p[X_1,\dots,X_5]$ tel que $f=g'(L_1',L_2')+ph$.

Considérons maintenant le système suivant :

$$\begin{cases} L_1'(x_1,\dots,x_5)\equiv 0 \pmod p\,,\\ L_2'(x_1,\dots,x_5)\equiv 0 \pmod p\,,\\ h(x_1,\dots,x_5)\equiv 0 \pmod p\,. \end{cases}$$

On a $\deg h+\deg L_1'+\deg L_2'\le 4$. Le théorème de Chevalley–Warning permet d'affirmer l'existence d'une solution primitive $(x_1,\dots,x_5)$ de ce système. Cette solution vérifie $f(x_1,\dots,x_5)\equiv 0 \pmod{p^2}$.

4. Les polynômes de degré 3 sans terme constant

4.1. Lemme. *Soient K un corps commutatif dont le nombre des éléments est supérieur ou égal à trois, et $f\in K[X_1,\dots,X_n]$ un polynôme singulier de la forme $f=f_3+f_2$, où f_i est une forme homogène de degré i. Alors f peut s'écrire sous la forme $f=g(L_1,\dots,L_k)$ où les L_i sont des formes de degré 1 et g un élément de $K[X_1,\dots,X_k]$, de degré 3 et anisotrope sur K.*

P r e u v e. Si f est anisotrope, on pose $g=f$ et $L_i=X_i$. Sinon, considérons $(a_1,\dots,a_n)\ne(0,\dots,0)$ tel que $f(a_1,\dots,a_n)=0$. Il existe une transformation linéaire inversible et homogène des variables $X_i=\sum_{1\le j\le n} l_{ij}Y_j$ telle que $(0,\dots,0,1)$ soit l'image de $(a_1,\dots,a_n)$.

En posant $f(X_1,\dots,X_n)=h(Y_1,\dots,Y_n)$, on a $h(0,\dots,0,1)=0$. Le polynôme $h(Y_1,\dots,Y_n)$ s'écrit sous la forme

$$\begin{aligned} h(Y_1,\dots,Y_n)=a_nY_n^3+Y_n^2(a_1Y_1+\dots+a_{n-1}Y_{n-1})+Y_nq(Y_1,\dots,Y_{n-1})\\ +b_nY_n^2+Y_n(b_1Y_1+\dots+b_{n-1}Y_{n-1})+g(Y_1,\dots,Y_{n-1})\,, \end{aligned}$$

où $q(Y_1,\dots,Y_{n-1})$ est une forme quadratique. On a

$$h(0,\dots,0,1)=a_n+b_n=0\,. \tag{3}$$

Comme f est singulier, alors il en est de même pour h, d'où

$$\frac{\partial h}{\partial Y_n}(0,\dots,0,1) = 3a_n + 2b_n = 0\,. \tag{4}$$

Les relations (3) et (4) donnent $a_n = b_n = 0$. Donc

$$\begin{aligned} h(Y_1,\dots,Y_n) &= Y_n^2(a_1Y_1 + \dots + a_{n-1}Y_{n-1}) + Y_n q(Y_1,\dots,Y_n) \\ &\quad + Y_n(b_1Y_1 + \dots + b_{n-1}Y_{n-1}) + g(Y_1,\dots,Y_{n-1})\,. \end{aligned}$$

Par conséquent, pour tout $\alpha \in K$, on a $h(0,\dots,0,\alpha) = 0$.

Soit $\alpha \in K$ tel que $\alpha \neq 1$ et $\alpha \neq 0$; α existe car $\operatorname{card} K \geq 3$. La solution précédente de h nous donne le système

$$\begin{cases} \dfrac{\partial h}{\partial Y_i}(0,\dots,0,1) = a_i + b_i = 0 \\ \dfrac{\partial h}{\partial Y_i}(0,\dots,0,\alpha) = \alpha^2 a_i + \alpha b_i = 0 \end{cases} \quad \text{pour tout } 1 \leq i \leq n-1\,.$$

Il en résulte que $a_i = b_i = 0$ pour tout $1 \leq i \leq n-1$. Donc

$$h(Y_1,\dots,Y_n) = Y_n q(Y_1,\dots,Y_{n-1}) + g(Y_1,\dots,Y_{n-1})\,.$$

Si $q \neq 0$, il existe $(c_1,\dots,c_n) \in K^n$ tel que $q(c_1,\dots,c_{n-1}) \neq 0$, et $h(c_1,\dots,c_n) = 0$; dans ce cas $(c_1,\dots,c_n)$ est un zéro non singulier de h, ce qui est impossible, donc $q = 0$. Ceci entraîne que $h(Y_1,\dots,Y_n) = g(Y_1,\dots,Y_{n-1})$ et $f(X_1,\dots,X_n) = g(Y_1,\dots,Y_{n-1})$, avec g singulier comme f.

Si g n'est pas anisotrope, on répètera le même processus un nombre fini de fois tel qu'on aura $f(X_1,\dots,X_n) = g(Y_1,\dots,Y_k)$, avec g anisotrope.

Par ailleurs il existe une transformation linéaire telle que

$$Y_1 = L_1(X_1,\dots,X_n),\ \dots,\ Y_k = L_k(X_1,\dots,X_n)\,,$$

d'où $f = g(L_1,\dots,L_k)$.

4.2. Proposition. *Soit p un nombre premier impair. Alors pour tout polynôme f élément de $\mathbb{Z}_p[X_1,\dots,X_7]$, de degré trois et sans terme constant, l'équation $f(x_1,\dots,x_7) \equiv 0 \pmod{p^2}$ admet une solution primitive.*

Preuve. Considérons $F = \bar{f} \in \mathbb{F}_p[X_1,\dots,X_7]$.

1er cas : Si F est nul, alors il existe h élément de $\mathbb{Z}_p[X_1,\dots,X_7]$ tel que $f = ph$. D'après le théorème de Chevalley–Warning, $h \equiv 0 \pmod{p}$ admet une solution primitive $(x_1,\dots,x_7)$ et cette solution vérifie $f(x_1,\dots,x_7) \equiv 0 \pmod{p^2}$.

2ème cas : Si F est singulier, il existe $(x_1,\dots,x_7) \in \mathbb{F}_p^7$ et $1 \leq i_0 \leq 7$ tels que

$$F(x_1,\dots,x_7) = 0 \quad \text{et} \quad \frac{\partial F}{\partial X_{i_0}}(x_1,\dots,x_7) \neq 0\,.$$

D'après le lemme de Hensel, il existe $y = (y_1, \ldots, y_7) \in \mathbb{Z}_p^7$ primitif tel que $f(y_1, \ldots, y_7) = 0$, ce qui implique $f(y_1, \ldots, y_7) \equiv 0 \pmod{p^2}$.

$3^{\text{ème}}$ cas : Si F n'est pas singulier, écrivons F sous la forme $F = F_3 + F_2 + F_1$, où les F_i sont les composantes homogènes de F. D'après la proposition 2.1, $F_1 = 0$. D'où, d'après le lemme précédent, F peut s'écrire sous la forme $F = g(L_1, \ldots, L_k)$, où g est un polynôme anisotrope et les L_i des formes linéaires. D'après le théorème de Chevalley–Warning, g dépend au plus de 3 variables, d'où

$$F(x_1, \ldots, x_7) = \begin{cases} g(L_1(x_1, \ldots, x_7), L_2(x_1, \ldots, x_7), L_3(x_1, \ldots, x_7)) & \text{ou} \\ g(L_1(x_1, \ldots, x_7), L_2(x_1, \ldots, x_7)) & \text{ou} \\ g(L_1(x_1, \ldots, x_7))\,. \end{cases}$$

Soit $g' \in \mathbb{Z}_p[X_1, \ldots, X_k]$ ($k = 1, 2$ ou 3), de degré 3 tel que $\overline{g}' = g$. Soient $L'_1 \in \mathbb{Z}_p[X_1, \ldots, X_7]$ des formes linéaires ($i = 1, 2, 3$) telles que $\overline{L}'_i = L_i$. Considérons $G \in \mathbb{Z}_p[X_1, \ldots, X_7]$ tel que

$$f = g'(L'_1, \ldots, L'_k) + pG\,.$$

Le système suivant :

$$\begin{cases} L'_1(x_1, \ldots, x_7) \equiv 0 \pmod{p}, \\ \ldots \\ L'_k(x_1, \ldots, x_7) \equiv 0 \pmod{p} \quad (k = 1, 2 \text{ ou } 3), \\ G(x_1, \ldots, x_7) \equiv 0 \pmod{p}, \end{cases}$$

admet une solution primitive $(x_1, \ldots, x_7) \in \mathbb{Z}_p^7$ puisqu'il vérifie les hypothèses du théorème de Chevalley–Warning. Cette solution vérifie $f(x_1, \ldots, x_7) \equiv 0 \pmod{p^2}$, d'où la proposition.

Le contre-exemple suivant montre que la proposition précédente ne peut être étendue au cas de $p = 2$.

Soit $f(X, Y) = X^2Y + XY^2 + X^2 + Y^2 + XY \in \mathbb{Z}_2[X, Y]$. Pour tout $(x, y) \in \mathbb{Z}_2^2$ avec x ou y non divisible par 2, on a $f(x, y) \equiv 1 \pmod{4}$.

Soit $g(X, Y) = X^2 + XY + Y^2 \in \mathbb{Z}_2[X, Y]$. Pour tout $(x, y) \in \mathbb{Z}_2$ on a $g(x, y) \equiv f(x, y) \pmod{2}$. Posons

$$F = f(X_1, X_2) + f(X_3, X_4) + f(X_5, X_6),$$
$$G = g(X_1, X_2) + g(X_3, X_4) + g(X_5, X_6)\,,$$

et considérons le polynôme

$$H = F + X_7G + X_7^2\,.$$

Montrons que si $H(x_1, \ldots, x_7) \equiv 0 \pmod{4}$, alors $x_1 \equiv \ldots \equiv x_7 \equiv 0 \pmod{2}$.

Pour cela considérons d'abord le cas où $x_7 \equiv 0 \pmod{2}$; alors

$$H(x_1, \ldots, x_7) \equiv F(x_1, \ldots, x_6) \equiv 0 \pmod{2}\,,$$

d'où $G(x_1,\dots,x_6)\equiv 0 \pmod 2$, ce qui implique

$$x_7G(x_1,\dots,x_6)\equiv 0 \pmod 4.$$

Par conséquent $F(x_1,\dots,x_6)\equiv 0 \pmod 4$, d'où $x_1\equiv\dots\equiv x_6\equiv 0 \pmod 2$.

Considérons maintenant le cas $x_7\equiv 1 \pmod 2$; dans ce cas on a

$$H(x_1,\dots,x_7)\equiv F(x_1,\dots,x_6)+G(x_1,\dots,x_6)+1\equiv 0 \pmod 2,$$

d'où $F(x_1,\dots,x_6)+G(x_1,\dots,x_6)\equiv 1 \pmod 2$, ce qui est impossible car

$$\begin{aligned}&F(x_1,\dots,x_6)+G(x_1,\dots,x_6)\\&\quad=f(x_1,x_2)+g(x_1,x_2)+\dots+f(x_5,x_6)+g(x_5,x_6)\equiv 0 \pmod 2\end{aligned}$$

pour tout $(x_1,\dots,x_6)\in\mathbb{Z}_2^6$.

5. La construction des polynômes de degré $d\geq 4$ anisotropes modulo 4

5.1. Proposition. *Pour tout $n\in\mathbb{N}^*$,*

$$F_n=\sum_{\substack{1\leq i_1<\dots<i_k\leq n\\ k\geq 1}} X_{i_1}\dots X_{i_k}=\prod_{j=1}^{n}(X_j+1)-1$$

et $F_n(x_1,\dots,x_n)\equiv 1 \pmod 2$ pour tout $(x_1,\dots,x_n)\in\mathbb{Z}^n$ tel que l'un des x_i soit impair.

Preuve. $F_n(X_1,\dots,X_n)=\prod_{j=1}^{n}(X_j+1)-1$ se démontre trivialement par récurrence. Considérons $(x_1,\dots,x_n)\in\mathbb{Z}^n$ tel que l'un des x_i soit impair. Sans perte de généralité supposons que c'est x_1; on a alors

$$F_n(x_1,\dots,x_n)=\prod_{j=1}^{n}(x_j+1)-1\equiv -1\equiv 1 \pmod 2.$$

5.2. Lemme. *Soit n un entier supérieur ou égal à 2. Pour tout $(x_1,\dots,x_n)\in\mathbb{Z}^n$ on a*

$$x_1^2\dots x_n^2\equiv G_n(x_1,\dots,x_n) \pmod 4,$$

où

$$G_n(X_1,\dots,X_n)=X_1\dots X_n(X_1+\dots+X_n-n+1).$$

Preuve. Pour tout $(x_1,x_2)\in\mathbb{Z}^2$, on a $x_1^2x_2^2\equiv x_1^2x_2+x_1x_2^2-x_1x_2 \pmod 4$, d'où le lemme est vérifié pour $n=2$.

Supposons que $x_1^2\dots x_n^2\equiv G_n(x_1,\dots,x_n) \pmod 4$ pour tout $(x_1,\dots,x_n)\in\mathbb{Z}^n$. Alors pour tout $(x_1,\dots,x_{n+1})\in\mathbb{Z}^{n+1}$, on a

$$\begin{aligned}x_1^2\dots x_{n+1}^2&\equiv x_1\dots x_n(x_1+\dots+x_n-n+1)x_{n+1}^2 \pmod 4\\&\equiv x_1^2x_{n+1}^2x_2\dots x_n+\dots+x_1\dots x_{n-1}x_n^2x_{n-1}^2\\&\quad-(n-1)x_1\dots x_nx_{n+1}^2 \pmod 4.\end{aligned}$$

En remplaçant $x_i^2 x_{n+1}^2$ par $x_i^2 x_{n+1} + x_i x_{n+1}^2 - x_i x_{n+1}$ pour $i = 1, \dots, n$ dans l'expression précédente on obtient la propriété désirée pour le rang n+1.

5.3. Théorème. *Pour tout entier n supérieur ou égal à 1 il existe un polynôme $f_n \in \mathbb{Z}[X_1, \dots, X_n]$ de degré $n+1$ sans terme constant tel que pour tout $(x_1, \dots, x_n) \in \mathbb{Z}^n$, on a*

$$f_n(x_1, \dots, x_n) \equiv (F_n(x_1, \dots, x_n))^2 \pmod 4,$$

où F_n est le polynôme de la proposition 5.1.

Preuve. D'après la proposition 5.1, pour tout $(x_1, \dots, x_n) \in \mathbb{Z}^n$ on a

$$F_n(x_1, \dots, x_n) = x_1 \dots x_n + \sum_{1 \le i_1 < \dots < i_{n-1} \le n} x_{i_1} \dots x_{i_{n-1}} + \dots + \sum_{i=1}^{n} x_i .$$

D'où

$$(F_n(x_1, \dots, x_n))^2 = x_1^2 \dots x_n^2 + \sum_{k=1}^{n-1} \sum_{1 \le i_1 < \dots < i_k \le n} x_{i_1}^2 \dots x_{i_k}^2 + 2 \sum_{\substack{k=1 \\ k'=1}}^{n} \sum_{\substack{1 \le i_1 < \dots < i_k \le n \\ 1 \le j_1 < \dots < j_{k'} \le n \\ \{i_1, \dots, i_k\} \ne \{j_1, \dots, j_{k'}\}}} x_{i_1} \dots x_{i_k} x_{j_1} \dots x_{j_{k'}} .$$

D'après le lemme précédent on a $x_{i_1}^2 \dots x_{i_k}^2 \equiv G_k(x_{i_1}, \dots, x_{i_k}) \pmod 4$, où $G_k \in \mathbb{Z}[X_1, \dots, X_k]$ est de degré $k+1$ et sans terme constant, ce qui nous donne

$$\sum_{k=1}^{n-1} \sum_{1 \le i_1 < \dots < i_k \le n} x_{i_1}^2 \dots x_{i_k}^2 \equiv \sum_{k=1}^{n-1} \sum_{1 \le i_1 < \dots < i_k \le n} G_k(x_{i_1}, \dots, x_{i_k}) \pmod 4 .$$

Pour $k = n$ on a

$$x_1^2 \dots x_n^2 \equiv G_n(x_1, \dots, x_n) \pmod 4 .$$

D'autre part, $x^k \equiv x \pmod 2$ pour tout $(x, k) \in \mathbb{Z} \times \mathbb{N}^*$. Dès lors, en remplaçant dans le polynôme

$$\sum_{\substack{k=1 \\ k'=1}}^{n} \sum_{\substack{1 \le i_1 < \dots < i_k \le n \\ 1 \le j_1 < \dots < j_{k'} \le n}} X_{i_1} \dots X_{i_k} X_{j_1} \dots X_{j_{k'}}$$

les exposants des indéterminées par 1, on obtient un polynôme $H_n \in \mathbb{Z}[X_1, \dots, X_n]$ de degré n sans terme constant et tel que pour tout $(x_1, \dots, x_n) \in \mathbb{Z}^n$,

$$\sum_{\substack{k=1 \\ k'=1}}^{n} \sum_{\substack{1 \le i_1 < \dots < i_k \le n \\ 1 \le j_1 < \dots < j_{k'} \le n}} x_{i_1} \dots x_{i_k} x_{j_1} \dots x_{j_{k'}} \equiv H_n(x_1, \dots, x_n) \pmod 2 ,$$

ce qui équivaut à

$$2\sum_{\substack{k=1\\k'=1}}^{n}\ \sum_{\substack{1\le i_1<\ldots<i_k\le n\\1\le j_1<\ldots<j_{k'}\le n}} x_{i_1}\ldots x_{i_k}x_{j_1}\ldots x_{j_{k'}} \equiv 2H_n(x_1,\ldots,x_n) \pmod 4\,.$$

Finalement, on pose

$$f_n = G_n + \sum_{k=1}^{n-1}\ \sum_{1\le i_1<\ldots<i_k\le n} G_k(X_{i_1},\ldots,X_{i_k}) + 2H_n$$

et on voit aisément que pour tout $(x_1,\ldots,x_n)\in\mathbb{Z}^n$, on a

$$f_n(x_1,\ldots,x_n)\equiv (F_n(x_1,\ldots,x_n))^2 \pmod 4 \quad\text{et}\quad \deg f_n = \deg G_n = n+1\,,$$

d'où le théorème.

5.4. Corollaire. *Pour tout $n\in\mathbb{N}$ supérieur ou égal à 1, il existe $F\in\mathbb{Z}[X_1,\ldots,X_{3n}]$ sans terme constant, de degré $n+1$ et anisotrope modulo 4.*

P r e u v e. On considère le polynôme

$$F(X_1,\ldots,X_{3n}) = f_n(X_1,\ldots,X_n) + f_n(X_{n+1},\ldots,X_{2n}) + f_n(X_{2n+1},\ldots,X_{3n})\,,$$

où f_n est le polynôme du théorème précédent. Il est clair que F est anisotrope modulo 4 et $\deg F = \deg f_n = n+1$.

On a $2\deg F + 1 = 2(n+1)+1 \le 3n$ pour tout $n\ge 3$, ainsi le corollaire précédent avec le contre-exemple de la fin du paragraphe 4 permettent de conclure que $p(d) > 2$ pour tout $d\ge 3$.

6.1. Construction des polynômes homogènes de degré D multiple de p^2-p, anisotropes modulo p^2 ($p\ne 2$)

6.1. Proposition. *Pour tout nombre premier $p>2$, le polynôme*

$$V(X_1,X_2) = (X_1^p - X_2^{p-1}X_1)^{p-1} + X_2^{p^2-p}$$

vaut 1 modulo p^2 pour tout $(x_1,x_2)\in\mathbb{Z}^2$ tel que x_1 ou x_2 soit non divisible par p.

P r e u v e. Soit $(x_1,x_2)\in\mathbb{Z}^2$ tel que x_1 ou x_2 soit non divisible par p. Si p divise x_2, alors p ne divise pas x_1 et

$$V(x_1,x_2)\equiv x_1^{p^2-p}\equiv 1 \pmod{p^2}\,.$$

Si p divise x_1, alors p ne divise pas x_2; on a alors

$$V(x_1,x_2)\equiv x_2^{p^2-p}\equiv 1 \pmod{p^2}\,.$$

Supposons que p ne divise ni x_1 ni x_2; on a $x_2^{p-1} \equiv 1 \pmod p$, d'où $x_1^p - x_2^{p-1}x_1 \equiv x_1 - x_1 \equiv 0 \pmod p$. On en déduit que $(x_1^p - x_2^{p-1}x_1)^{p-1} \equiv 0 \pmod{p^2}$ puisque $p-1 \geq 2$. Ainsi on a

$$V(x_1, x_2) \equiv x_2^{p^2-p} \equiv 1 \pmod{p^2}\,.$$

6.2. Corollaire. *Pour tout nombre premier $p > 2$ et pour tout $d \in \mathbb{N}^*$, le polynôme*

$$f(X_1, \ldots, X_{2d}) = V(n_d(X_1, \ldots, X_d), n_d(X_{d+1}, \ldots, X_{2d}))$$

vaut 1 modulo p^2 pour tout $(x_1, \ldots, x_{2d})$ tel que l'un des x_i soit non divisible par p (n_d est une forme normique de degré d à coefficients dans $\mathbb{Z}_p$). Le degré de f est égal à $d(p^2-p)$.

Preuve. Soit $(x_1, \ldots, x_{2d}) \in \mathbb{Z}^{2d}$ tel que l'un des x_i soit non divisible par p; alors $n_d(x_1, \ldots, x_d)$ ou $n_d(x_{d+1}, \ldots, x_{2d})$ n'est pas divisible par p et d'après la proposition précédente

$$f(x_1, \ldots, x_{2d}) = V(n_d(x_1, \ldots, x_d), n_d(x_{d+1}, \ldots, x_{2d})) \equiv 1 \pmod{p^2}\,.$$

6.3. Proposition. *Pour tout $D \in \mathbb{N}^*$ multiple de $p^2 - p$, où p est un nombre premier > 2, il existe un polynôme homogène $F \in \mathbb{Z}[X_1, \ldots, X_n]$ de degré D, tel que $n \geq 2D+1$, et anisotrope modulo p^2.*

Preuve. Il existe $d \in \mathbb{N}^*$ tel que $D = d(p^2-p)$. D'après le corollaire 6.2, il existe $f(X_1, \ldots, X_{2d})$ de degré D qui vaut 1 modulo p^2 pour tout $(x_1, \ldots, x_{2d})$ dont l'un des x_i est non divisible par p. Posons

$$F(X_1, \ldots, X_n) = f(X_1, \ldots, X_{2d}) + \ldots + f(X_{2d(p^2-2)+1}, \ldots, X_{2d(p^2-1)})$$

avec $n = 2d(p^2-1) > 2D$. Pour tout $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ dont l'un des x_i est non divisible par p, on a

$$F(x_1, \ldots, x_n) \equiv k \pmod{p^2}, \quad \text{avec } 1 \leq k \leq p^2 - 1\,.$$

Donc $F(X_1, \ldots, X_n)$ est anisotrope modulo p^2.

7. Construction des polynômes homogènes de degré D multiple de 4, anisotropes modulo 4. Soit le polynôme

$$\begin{aligned} f(X_1, X_2, X_3) = {} & X_1^2X_2X_3 + X_2^2X_1X_3 + X_3^2X_1X_2 \\ & + X_1^2X_2^2 + X_1^2X_3^2 + X_2^2X_3^2 - X_1^4 - X_2^4 - X_3^4\,, \end{aligned}$$

découvert par Terjanian [3]. On sait que pour tout $(x_1, x_2, x_3) \in \mathbb{Z}^3$ tel que l'un des x_i soit impair, $f(x_1, x_2, x_3) \equiv 3 \pmod 4$.

7.1. Proposition. *Pour tout $d \in \mathbb{N}^*$ le polynôme $F(X_1, \ldots, X_{3d}) = f(n_d(X_1, \ldots, X_d), n_d(X_{d+1}, \ldots, X_{2d}), n_d(X_{2d+1}, \ldots, X_{3d}))$ est de degré $4d$ et vaut 3 modulo 4 pour tout $(x_1, \ldots, x_{3d})$ tel que l'un des x_i soit impair (où n_d est une forme normique de degré d à coefficients dans $\mathbb{Z}_p$).*

P r e u v e. Soit $(x_1,\dots,x_{3d})\in\mathbb{Z}^{3d}$ tel que l'un des x_i soit impair; on peut supposer que c'est x_1, d'où $n_d(x_1,\dots,x_d)$ est impair, et par conséquent

$$\begin{aligned}F(x_1,\dots,x_{3d}) &= f(n_d(x_1,\dots,x_d),n_d(x_{d+1},\dots,x_{2d}),n_d(x_{2d+1},\dots,x_{3d}))\\ &\equiv 3 \pmod 4.\end{aligned}$$

On a $\deg f=4$ et $\deg n_d=d$, où $\deg F=4d$.

7.2. Corollaire. *Pour tout $D\in\mathbb{N}^*$ multiple de 4, il existe un élément de $\mathbb{Z}[X_1,\dots,X_n]$ homogène de degré D et anisotrope modulo 4, où $n=9D/4$.*

P r e u v e. On a $D=4d$, $d\in\mathbb{N}^*$. D'après la proposition précédente il existe $F(X_1,\dots,X_{3d})\in\mathbb{Z}[X_1,\dots,X_{3d}]$ de degré D qui vaut 3 modulo 4 pour tout $(x_1,\dots,x_{3d})$ dont l'un des x_i est impair. Pour $n=9d=9D/4$, posons

$$f(X_1,\dots,X_n)=F(X_1,\dots,X_{3d})+F(X_{3d+1},\dots,X_{6d})+F(X_{6d+1},\dots,X_{9d}).$$

Pour tout $(x_1,\dots,x_n)$ dont l'un des x_i est impair, on a $f(x_1,\dots,x_n)\equiv k \pmod 4$, où k prend les valeurs 3, 6 ou 9. On en déduit que $f(X_1,\dots,X_n)$ est anisotrope modulo 4.

Le corollaire 7.2 nous amène à la question suivante : Existe-t-il des polynômes homogènes éléments de $\mathbb{Z}[X_1,\dots,X_{2d+1}]$ de degré d non multiple de 4 et anisotrope modulo 4?

BIBLIOGRAPHIE

[1] J. Ax and S. Kochen, *Diophantine problems over local fields I*, Amer. J. Math. 87 (1965), 605–630.

[2] —, —, *Diophantine problems over local fields: III. Decidable fields*, Ann. of Math. 83 (1966), 437–456.

[3] G. Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A 262 (1966), 612.

LABORATOIRE D'ALGÈBRE
UNIVERSITÉ PAUL SABATIER
118 ROUTE DE NARBONNE
31062 TOULOUSE CEDEX, FRANCE

Reçu par la Rédaction le 14.1.1991;
en version modifiée le 20.5.1992