SÉMINAIRE N. BOURBAKI

JEAN-PIERRE AZRA

Relations diophantiennes et la solution négative du 10e problème de Hilbert

Séminaire N. Bourbaki, 1971, exp. n° 383, p. 11-28

<http://www.numdam.org/item?id=SB_1970-1971__13__11_0>

© Association des collaborateurs de Nicolas Bourbaki, 1971, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques

http://www.numdam.org/

Séminaire BOURBAKI
23e année, 1970/71, n° 383 Novembre 1970

RELATIONS DIOPHANTIENNES ET LA SOLUTION NÉGATIVE DU 10e PROBLÈME DE HILBERT

(d'après M. DAVIS, H. PUTNAM, J. ROBINSON et I. MATIASEVITCH)

par Jean-Pierre AZRA

0. Introduction.

Le 10e Problème de Hilbert [1] (c'est-à-dire le problème de trouver un procédé effectif uniforme permettant de dire, étant donné un polynôme $P(x_1,x_2,\ldots,x_n)$ dont les coefficients sont des entiers relatifs, s'il existe ou non des entiers $a_1,a_2,\ldots,a_n$ tels que $P(a_1,a_2,\ldots,a_n) = 0$) a reçu une réponse négative grâce aux travaux de M. Davis, H. Putnam, J. Robinson ([2] et [3]) et tout récemment de I. Matiasevitch [4].

La théorie des fonctions récursives, dont on trouvera un exposé général dans [5], permet de donner des équivalents mathématiques précis aux notions "périmathématiques" (c.à.d. naïves) de "procédé effectif uniforme" et de "relation effectivement décidable", ce qui donnera un sens aux théorèmes suivants (voir le théorème III.1 et le paragraphe IV).

THÉORÈME 0.1.- Il n'existe pas de procédé effectif uniforme pour décider si une équation diophantienne donnée a ou non des solutions.

THÉORÈME 0.2.- Pour toute relation effectivement décidable $R(x_1,\ldots,x_p)$, il existe un polynôme $P(x_1,\ldots,x_p,y_1,\ldots,y_n)$, dont les coefficients sont des entiers relatifs, tel que le p-uplet $(x_1,\ldots,x_p)$ satisfait R si et seulement si $\exists\, y_1 \ldots \exists\, y_n \quad P(x_1,\ldots,x_p,y_1,\ldots,y_n) = 0$.

Remarquons tout de suite qu'il importe peu que les solutions d'une équation diophantienne soient cherchées dans l'ensemble $\mathbb{Z}$ des entiers relatifs, dans l'ensemble $\mathbb{N}$ des entiers naturels ou dans l'ensemble $\mathbb{N}^+$ des entiers > 0 . Ne consi-

dérons, pour simplifier, que des équations à une seule inconnue. L'équation $P(x) = 0$ a des solutions dans $\mathbb{N}$ si et seulement si l'équation $P(x_1^2 + x_2^2 + x_3^2 + x_4^2) = 0$ a des solutions dans $\mathbb{Z}$ (car d'après le Théorème de Lagrange tout nombre positif est une somme de quatre carrés) ; l'équation $P(x) = 0$ a des solutions dans $\mathbb{N}^+$ si et seulement si l'équation $P(x + 1) = 0$ a des solutions dans $\mathbb{N}$; enfin l'équation $P(x) = 0$ a des solutions dans $\mathbb{Z}$ si et seulement si l'équation $P(x).P(0).P(-x) = 0$ a des solutions dans $\mathbb{N}^+$. Il est clair que le passage d'un cas à un autre s'effectue par une transformation effectivement réalisable de l'équation proposée. Pour des raisons techniques c'est le cas des solutions dans $\mathbb{N}^+$ que nous étudierons.

L'ordre suivi dans cet exposé ne respecte pas l'ordre chronologique dans lequel les résultats ont été démontrés. Il semble que ce soit A. Tarski qui ait eu le premier l'idée d'étudier les relations diophantiennes et qui en ait donné la caractérisation I.1. Le premier progrès vraiment significatif dans l'étude des relations diophantiennes est dans [2] ; dans cet article pour une part puis dans [3] pour le reste, paraît la démonstration de II.9 et II.10, sous forme en quelque sorte "conditionnelle", les auteurs de [3] n'ayant pas su prouver que le graphe de la fonction exponentielle est diophantien. Ces résultats partiels ont tout de même permis à M. Davis, H. Putnam et J. Robinson de publier dans [3] la belle solution négative du problème de la décision pour les équations diophantiennes à exposants variables, solution reprise pour l'essentiel dans le paragraphe III du présent exposé. Le dernier maillon apparaît enfin dans [4] : I. Matiasevitch montre que $y = u_{2x}$, où u_n est le n-ième terme de la suite de Fibonacci, est diophantienne. Or la fonction $y = u_{2x}$ croît "en gros" comme la fonction exponentielle, ce qui d'après un théorème de [2] montre que le graphe de la fonction exponentielle est diophantien.

Dans notre exposé, nous suivrons [7] pour la démonstration de II.1 et de II.10 : la démonstration de II.1 fait usage des suites de Lucas au lieu de celle de Fibonacci, et celle de II.10 est directe.

La propriété : "tout sous-ensemble diophantien de $\mathbb{N}^+$ est l'ensemble des valeurs positives d'un certain polynôme" figure dans [6].

Aucune propriété fine de l'arithmétique des nombres entiers n'est utilisée dans les démonstrations. Par contre, il est fait un usage constant du

"THÉORÈME CHINOIS".- Soient $p_1, p_2, \ldots, p_m$ premiers entre eux deux à deux. Alors, quels que soient $z_1, \ldots, z_m$ il existe a tel que $a \equiv z_i \pmod{p_i}$ pour tout i tel que $1 \leq i \leq m$.

Les notations utilisées, notamment en ce qui concerne les symboles logiques, sont celles de [5].

I. Relations diophantiennes.

D'après les remarques faites dans le paragraphe précédent, les arguments des relations que nous considérons à partir de maintenant sont supposés décrire $\mathbb{N}^+$. Nous nous autoriserons les abus de langage usuels, comme ceux qui sont contenus dans la définition suivante :

> Soit f une application de $(\mathbb{N}^+)^p$ dans $\mathbb{N}^+$; nous appellerons graphe de f la relation $f(x_1, \ldots, x_p) = y$.

DÉFINITION.- Une relation $R(x_1, \ldots, x_p)$ est dite diophantienne s'il existe un entier $n \geq 0$ et un polynôme $P(x_1, \ldots, x_p, y_1, \ldots, y_n)$ à coefficients dans $\mathbb{Z}$ tel que, pour tout $x_1, \ldots, x_p \in \mathbb{N}^+$, $R(x_1, \ldots, x_p)$ si et seulement si $\exists\, y_1 \ldots \exists\, y_n$ $(P(x_1, \ldots, x_p, y_1, \ldots, y_n) = 0)$.

On déduit aisément de la définition la caractérisation suivante :

PROPOSITION I.1.- Pour qu'une relation soit diophantienne, il faut et il suffit qu'elle puisse être obtenue à partir des graphes de l'addition et de la multiplication sur $\mathbb{N}^+$ par un nombre fini, effectué dans un ordre quelconque, de conjonctions, disjonctions, quantifications existentielles et changements de variables.

COROLLAIRE I.2.- La relation obtenue à partir d'une relation diophantienne en substituant à ses arguments des fonctions de graphe diophantien est diophantienne.

Exemples.- La relation $x \equiv y \pmod{z}$ qui équivaut à $\exists\, t(x - y - (t-1)z = 0) \vee \exists\, t(y - x - tz = 0)$ est diophantienne. Donc la relation $x|y$ (x divise y) est diophantienne. La relation $x < y$ qui équivaut à $\exists\, z\,(x + z - y = 0)$, la relation $x \neq y$ qui équivaut à $x < y \vee y < x$ sont diophantiennes. Nous montrerons plus loin qu'il existe des relations diophantiennes dont la négation n'est pas diophantienne.

II. Les exemples fondamentaux de relations diophantiennes.

La définition diophantienne de l'exponentielle.

Soient, pour $a \in \mathbb{N}^+$, $x_n(a)$ et $y_n(a)$ les suites ("de Lucas") définies par les relations de récurrence

$$(1) \qquad \begin{aligned} x_{n+1}(a) &= 2ax_n(a) - x_{n-1}(a) \\ y_{n+1}(a) &= 2ay_n(a) - y_{n-1}(a) \end{aligned} \qquad (n \in \mathbb{Z})$$

avec des conditions qui déterminent les deux suites :

$$x_o(a) = 1 \qquad x_1(a) = a$$

$$y_o(a) = 0 \qquad y_1(a) = 1 \ .$$

Il est connu que $x_n^2(a) - (a^2 - 1)y_n^2(a) = 1$, et qu'inversement si $x > 0$ et y vérifient l'équation de Pell $x^2 - (a^2 - 1)y^2 = 1$, il existe un entier $n \in \mathbb{Z}$ tel que $x = x_n(a)$ et $y = y_n(a)$. On a d'ailleurs pour tout $n \in \mathbb{Z}$:

$$x_n + y_n\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^n \ .$$

On en déduit immédiatement les conséquences suivantes (on écrit x_n , y_n pour $x_n(a)$, $y_n(a)$ chaque fois que le contexte le permet), qui sont valables pour tout choix des indices dans $\mathbb{Z}$:

$$(2) \qquad y_{m+n} = y_m x_n + x_m y_n$$

et en particulier :

$$y_{2k+1} = y_k x_{k+1} + x_k y_{k+1}$$

$$(3) \qquad x_{k+1} = ax_k + (a^2 - 1)y_k$$

(4) $y_{k+1} = x_k + ay_k$ (donc $y_{k+1} > y_k$).

(5) x_k et y_k sont premiers entre eux.

(6) $y_k \equiv k \pmod 2$ (6') $y_k \equiv k \pmod{a-1}$.

(7) $y_{-n} = -y_n$

(8) $n \mid t$ si et seulement si $y_n \mid y_t$

($y_n \mid y_{nk}$ se démontre par induction sur k à l'aide de (2), et inversement si $y_n \mid y_{nk+r}$ alors $y_n \mid y_r$ d'après (2) et (5)).

PROPOSITION II.1.- La relation (en u , v et a) $v = y_u(a)$ est diophantienne.

Il nous faut d'abord démontrer quelques lemmes.

LEMME II.2.- Si $a \equiv b \pmod c$, alors $y_n(a) \equiv y_n(b) \pmod c$.

Démonstration immédiate par induction sur n à l'aide de (1).

LEMME II.3.- (a) $y_{n+2k+1} \equiv y_n \pmod{y_{k+1} + y_k}$.

(b) $y_{n+2k+1} \equiv -y_n \pmod{y_{k+1} - y_k}$.

Démonstration : On montre d'abord par induction sur u que

$$y_{k+u} \mp y_{k+1-u} \pmod{y_{k+1} \pm y_k} ,$$

d'où le résultat en remplaçant u par $k + 1 + n$ et y_{-n} par $-y_n$.

Remarque.- Inversement, si $y_m \equiv y_n \pmod{y_{k+1} + y_k}$, alors $m \equiv n \pmod{2k+1}$. En effet, si $0 \leq m < n \leq k+1$, on a $0 \leq y_m < y_n < y_{k+1} + y_k$, donc $y_m \not\equiv y_n \pmod{y_{k+1} + y_k}$. Si $-k \leq m < 0 \leq n \leq k+1$, alors $0 < y_{-m} + y_n < y_{k+1} + y_k$, donc $y_m \not\equiv y_n \pmod{y_{k+1} + y_k}$.

LEMME II.4.- Si $2s + 1 \mid 2n + 1$, alors

(a) $y_{s+1} + y_s \mid y_{n+1} + y_n$;

(b) $y_{s+1} - y_s \mid y_{n+1} - y_n$.

Démontrons (b) à titre d'exemple : on a facilement $n \equiv s \pmod{2s+1}$, d'où $n = s + p(2s+1)$. Par II.3 :

$$y_{n+1} - y_n \equiv (-1)^p y_{s+1} - (-1)^p y_s \equiv 0 \pmod{y_{s+1} - y_s} .$$

LEMME II.5.- (a) $y_{2k+1} = (y_{k+1} + y_k)(y_{k+1} - y_k)$.

(b) $y_{k+1} + y_k$ et $y_{k+1} - y_k$ sont premiers entre eux.

(a) se démontre par simple calcul à l'aide de (2), (3) et (4).

(b) vient de (6), (4) et (5).

LEMME II.6.- $y_n^2 | y_{n.y_n}$ et inversement si $y_n^2 | y_t$, alors $y_n | t$.

Démonstration : en développant le binôme $(x_n + y_n\sqrt{a^2 - 1})^k = x_{nk} + y_{nk}\sqrt{a^2 - 1}$, on obtient $y_{nk} \equiv k x_n^{k-1} y_n \pmod{y_n^3}$, d'où $y_n^2 | y_{n.y_n}$.

Inversement, si $y_n^2 | y_t$, alors $n | t$ par (8). Soit $t = nk$, par la congruence ci-dessus on a $y_n | k x_n^{k-1}$, d'où $y_n | k$ par (5).

LEMME II.7.- Si $2n + 1 = (2s + 1)y_{2s+1}$, alors $(y_{s+1} \pm y_s)^2 | y_{n+1} \pm y_n$ et $y_{s+1} \pm y_s$ et $y_{n+1} \mp y_n$ sont premiers entre eux.

Démonstration : par II.6, $y_{2s+1}^2 | y_{2n+1}$, d'où, par II.5.(a) :

$$(y_{s+1} + y_s)^2 (y_{s+1} - y_s)^2 | (y_{n+1} + y_n)(y_{n+1} - y_n) .$$

Par II.4, on a $y_{s+1} \pm y_s | y_{n+1} \pm y_n$, d'où, par II.5.(b) : $(y_{s+1} \pm y_s)^2 | y_{n+1} \pm y_n$ et $y_{s+1} \pm y_s$ est premier avec $y_{n+1} \mp y_n$.

Démonstration de la proposition II.1 : soit $S(a,u,v)$ la relation $v = y_u(a) \wedge a > 1$ $(y , u , v \in \mathbb{N}^+)$. Nous allons montrer que, pour que $S(a,u,v)$ soit vraie, il faut et il suffit qu'il existe $p , q , g , h , m , x , y , z \in \mathbb{N}^+$ tels que les 13 relations suivantes soient simultanément vérifiées. Il s'en suivra par le paragraphe I que S est diophantienne, puis que $v = y_u(a)$ est diophantienne.

(A) $v \geq u$ (B) $p + (a-1)q > v$ (C) $a > 1$

(D) $p^2 - (a^2 - 1)q^2 = 1$ (E) $g^2 - (a^2 - 1)h^2 = 1$

(F) $(p + (a - 1)q)^2 | g + (a - 1)h$ (G) $(p + (a+1)q)^2 | g + (a + 1)h$

(H) $m \equiv 1 \pmod{p + (a - 1)q}$ (J) $m \equiv a \pmod{g + (a + 1)h}$

(K) $x^2 - (m^2 - 1)y^2 = 1$ (L) $z^2 - (a^2 - 1)v^2 = 1$

(M) $y \equiv u \pmod{p + (a - 1)q}$ (N) $y \equiv v \pmod{g + (a + 1)h}$.

Montrons d'abord que si $S(a,u,v)$ est vraie alors les 13 relations précédentes peuvent être simultanément satisfaites. Soit $z = x_u(a)$. On a évidemment (A), (C) et (L). Choisissons un s tel que $y_s(a) > y_u(a)$. Posons $p = x_s(a)$, $q = y_s(a)$. On a (B) et (D) trivialement. Comme $y_{2s+1}(a)$ est impair, il existe n tel que $2n + 1 = (2s + 1)y_{2s+1}(a)$. Posons $g = x_n(a)$, $h = y_n(a)$ qui satisfont (E) .

(F) et (G) sont vérifiées d'après II.7 (on a, par exemple, $p + (a - 1)q = y_{s+1} - y_s$ d'après (4)). Le même lemme montre aussi que $p + (a - 1)q$ et $g + (a + 1)h$ sont premiers entre eux. (H) et (J) peuvent alors être satisfaites grâce au Théorème Chinois.

Posons $x = x_u(m)$, $y = y_u(m)$ qui vérifient (K). Par (H), (J) et II.2, on obtient (M) et (N).

Inversement, supposons que a , u , v , p , q , g , h , m , x , y , $z \in \mathbb{N}^+$ vérifient les 13 relations (A) à (N). D'après (D), (E), (K) et (L), il existe s , k , n , $j \in \mathbb{N}^+$ tels que

$p = x_s(a)$ $g = x_k(a)$ $x = x_n(m)$ $z = x_j(a)$

$q = y_s(a)$ $h = y_k(a)$ $y = y_n(m)$ $v = y_j(a)$.

Par (F), (G) et (4) : $(y_{s+1}(a) \pm y_s(a))^2 \mid y_{k+1}(a) \pm y_k(a)$, d'où, par II.5.(a) : $y^2_{2s+1}(a) \mid y_{2k+1}(a)$, puis, par II.6 : $y_{2s+1}(a) \mid 2k + 1$, enfin, encore par II.5.(a) :

(9) $y_{s+1}(a) - y_s(a) \mid 2k + 1$.

Par (N), (J) et II.2 : $y_j(a) \equiv y_n(m) \equiv y_n(a) \pmod{y_{k+1}(a) + y_k(a)}$. Par la remarque qui suit le lemme II.3, on a donc $j \equiv n \pmod{2k + 1}$, donc, par (9)

(10) $j \equiv n \pmod{y_{s+1}(a) - y_s(a)}$.

Par (6') et (H) : $y_n(m) \equiv n \pmod{y_{s+1}(a) - y_s(a)}$. Par (M): $y_n(m) \equiv u \pmod{y_{s+1}(a) - y_s(a)}$, donc, par (10) : $j \equiv u \pmod{y_{s+1}(a) - y_s(a)}$. Or, par (A) et (B) : $u \leq y_j(a) < y_{s+1}(a) - y_s(a)$ et $j \leq y_j(a) < y_{s+1}(a) - y_s(a)$, donc finalement : $j = u$. C.Q.F.D.

PROPOSITION FONDAMENTALE II.8.- La relation $s = t^u$ est diophantienne.

Démonstration : nous nous servirons des propriétés élémentaires suivantes :

(11) $\quad x_n(a) - (a - t)y_n(a) \equiv t^n \pmod{2at - t^2 - 1}$

(12) $\quad x_n(a) \geq a^n$

(13) $\quad$ si $1 < t^n < a$, alors $t^n < 2at - t^2 - 1$.

Nous allons montrer que pour que $s = t^u$ il faut et il suffit qu'il existe $a , d , v , w , z \in \mathbb{N}^+$ tels que les relations (diophantiennes) suivantes soient simultanément vérifiées :

(A) $\quad v = y_u(a)$ $\qquad$ (B) $\quad z^2 - (a^2 - 1)v^2 = 1$

(C) $\quad s < 2at - t^2 - 1$ $\qquad$ (D) $\quad z - v(a - t) \equiv s \pmod{2at - t^2 - 1}$

(E) $\quad t < d$ $\qquad$ (F) $\quad u < d$

(G) $\quad 1 < a$ $\qquad$ (H) $\quad a^2 - (d^2 - 1)(d - 1)^2w^2 = 1$.

Supposons tout d'abord que $s = t^u$. On peut trouver d qui vérifie simultanément (E) et (F). (Donc $d > 1$.) Posons $a = x_{d-1}(d)$. Par (12) : $a \geq d^{d-1} > 1$, donc (G) est vérifiée. Par (6'), et parce que $a > 1$, il existe w qui vérifie (H). Choisissons $v = y_u(a)$, $z = x_u(a)$ de manière à satisfaire (A) et (B). (C) est vérifiée, d'après (12), (E), (F) et (13) si $s > 1$, directement si $s = 1$. Enfin (D) vient de (11).

Supposons inversement que $a , d , s , t , u , v , w , z \in \mathbb{N}^+$ vérifient les relations (A) à (H). Alors par (A) et (B) : $v = y_u(a)$ et $z = x_u(a)$. Par (D) et (11) :

(14) $\quad s \equiv t^u \pmod{2at - t^2 - 1}$.

Supposons d'abord que $t = 1$. Alors $s \equiv 1 \pmod{2(a - 1)}$, et par (C) : $s < 2(a - 1)$, donc $s = 1 = t^u$. Supposons donc maintenant que $t > 1$. Par (H) et (G), il existe $n \in \mathbb{N}^+$ tel que $a = x_n(d)$ et $(d - 1)w = y_n(d)$. Par (6'), $0 \equiv y_n(d) \equiv n \pmod{d - 1}$. Donc $n \geq d - 1$, donc, par (12), (E) et (F) et l'hypothèse $t > 1$: $a = x_n(d) \geq d^{d-1} > t^u > 1$. Par (13), on obtient donc $t^u < 2at - t^2 - 1$, d'où on déduit immédiatement à l'aide de (14) et de (C) que $s = t^u$.

C.Q.F.D.

Conséquences de la proposition II.8.

DÉFINITION.- Soient $k \in \mathbb{N}^+$, et α un rationnel $> k$. On pose

$$\binom{k}{\alpha} = \frac{\alpha(\alpha-1) \ldots (\alpha-k+1)}{k!} .$$

PROPOSITION II.9.- La relation (en a , b , p , q , k) $a/b = \binom{k}{p/q} \wedge p > qk$ est diophantienne.

Schéma de la démonstration :

Dans le (a), on fournit un système de trois relations (A), (B), (C) en a , b , p , q , k , x qui font intervenir une fonction auxiliaire F (dont il n'est exigé que de satisfaire certaines conditions *), telles que

$$a/b = \binom{k}{p/q} \wedge p > qk$$

si et seulement s'il existe un x tel que a , b , p , q , k , x vérifient simultanément (A), (B) et (C).

Dans le (b), ce résultat est utilisé pour montrer que la relation $a = \binom{k}{p} \wedge p > k$ est diophantienne. Ceci permet de montrer dans (c) que la relation $x = k!$ est diophantienne. Enfin dans (d), on construit une fonction F qui vérifie les conditions * , le (c) permettant de montrer que F a un graphe diophantien.

(a) Posons $p/q = \alpha$ $(\alpha > k)$, et développons $(1 + x^{-2})^{\alpha}$ en appliquant la formule de Taylor à l'ordre k à la fonction $f(t) = (1 + t)^{\alpha}$

$$x^{2k+1}(1 + x^{-2})^{\alpha} = \sum_{j=0}^{k} \binom{j}{\alpha} x^{-2j+2k+1} + \theta x^{-1} \alpha^{k+1} 2^{\alpha-1} \qquad \text{avec } 0 < \theta < 1 .$$

Soit $F(p,q,k)$ une fonction qui vérifie les conditions * suivantes :

* $\begin{cases} \text{Si on remplace } x \text{ par } F(p,q,k) \text{ les quantités} \\ \sum_{j=0}^{k} \binom{j}{\alpha} x^{-2j+2k+1} \quad \text{et} \quad \sum_{j=0}^{k-1} \binom{j}{\alpha} x^{-2j+2k-1} \quad \text{sont entières et} \\ x^{-1} \alpha^{k+1} 2^{\alpha-1} < 1 \qquad x^{-1} \alpha^{k} 2^{\alpha-1} < 1 . \end{cases}$

Alors, si l'on remplace x par $F(p,q,k)$, $[r]$ désignant la partie entière de r ,

$$[x^{2k+1}(1 + x^{-2})^{\alpha}] = \sum_{j=0}^{k} \binom{j}{\alpha} x^{-2j+2k+1}$$

$$[x^{2k-1}(1 + x^{-2})^{\alpha}] = \sum_{j=0}^{k-1} \binom{j}{\alpha} x^{-2j+2k-1} .$$

Or $\frac{1}{x} \sum_{j=0}^{k} \binom{j}{\alpha} x^{2(k-j)+1} - x \sum_{j=0}^{k-1} \binom{j}{\alpha} x^{2(k-j)-1} = \binom{k}{\alpha}$. Donc $a/b = \binom{k}{p/q} \wedge p > qk$ si et seulement s'il existe un $x \in \mathbb{N}^+$ tel que les trois relations suivantes soient simultanément vérifiées :

(A) $x = F(p,q,k)$ (B) $p > qk$

(C) $ax = b[x^{2k+1}(1 + x^{-2})^{\alpha}] - x^2 b[x^{2k-1}(1 + x^{-2})^{\alpha}]$.

On peut remarquer que la relation (en p , q , u , x et k) $u = [x^{2k+1}(1 + x^{-2})^{p/q}]$ équivaut à $x^{2p}u^q \leq x^{(2k+1)q}(1 + x^2)^p < x^{2p}(u + 1)^q$. Elle est donc diophantienne (par II.8, I.1 et I.2). Il en est de même pour $v = [x^{2k-1}(1 + x^{-2})^{p/q}]$.

Les relations (B) et (C), ci-dessus, sont donc diophantiennes.

(b) Posons $b = q = 1$ dans les relations précédentes, et prenons, pour $F(p,1,k)$, la fonction $p^{k+1}2^p$ (qui satisfait évidemment les conditions *) dont le graphe est diophantien par II.8 et I.2. La relation $p > k \wedge a = \binom{k}{p}$ est donc diophantienne.

(c) Il est facile de montrer en se servant de (b) - comme on l'a fait dans (a) pour montrer que la relation $u = [x^{2k+1}(1 + x^{-2})^{p/q}]$ est diophantienne - que la relation $u = \left[\frac{p^k}{\binom{k}{p}}\right] \wedge p > k$ est diophantienne. Or on peut montrer que $k! = \left[\frac{p^k}{\binom{k}{p}}\right]$ pour $p > (2k)^{k+1}$. On en déduit immédiatement que la relation $x = k!$ est diophantienne.

(d) Si $\alpha = \frac{p}{q}$, on a $\binom{j}{\alpha} = \frac{p(p-q)(p-2q)\ \ldots\ (p-(j-1)q)}{q^j.j!}$, donc, si on choisit x multiple de $q^k.k!$, les quantités $\sum_{j=0}^{k} \binom{j}{p/q} x^{-2j+2k+1}$ et $\sum_{j=0}^{k-1} \binom{j}{p/q} x^{-2j+2k-1}$ sont entières. D'autre part, si on choisit x multiple de $p^{k+1}2^p$, les conditions $x^{-1}(p/q)^{k+1}2^{(p/q)-1} < 1$ et $x^{-1}(p/q)^k 2^{(p/q)-1} < 1$ sont réalisées. Finalement, si on choisit $F(p,q,k) = q^k.k!.p^{k+1}2^p$, les conditions * sont toutes réalisées. Or, par II.8, II.9.(c) et I.2, le graphe de F est diophantien. Donc, par les résultats de (a), la relation $a/b = \binom{k}{p/q} \wedge p > qk$ est diophantienne.

C.Q.F.D.

COROLLAIRE II.10.- Les relations $y = x!$, $z = \prod_{j \leq y} (a - j)$, $z = \prod_{k \leq y} (1 + kt)$ sont diophantiennes.

Démonstration : pour obtenir les deux dernières relations, substituer des expressions convenables aux arguments de la relation qui figure dans l'énoncé de II.9.

III. Relations récursivement énumérables.

DÉFINITION.- Une relation est dite récursivement énumérable si elle peut être obtenue à partir des graphes de l'addition et de la multiplication sur $\mathbb{N}^+$ par un nombre fini, effectué dans un ordre quelconque, de conjonctions, disjonctions, quantifications existentielles, quantifications universelles bornées et changements de variables.

De la proposition I.1, on déduit trivialement que toute relation diophantienne est récursivement énumérable. La réciproque de cette propriété constitue le résultat principal de la théorie des relations diophantiennes.

THÉORÈME III.1.- Toute relation récursivement énumérable est diophantienne.

Il suffit évidemment de prouver que si la relation S est obtenue à partir de la relation diophantienne R par quantification universelle bornée, alors S est diophantienne. Nous aurons besoin de quelques lemmes dont la démonstration est immédiate :

LEMME III.2.- Soient $k \geq 1$, $n \geq 1$, $d > 1$ tels que d divise $1 + kn!$. Alors $n < d$.

LEMME III.3.- Si $n > 1$, les n entiers $1 + jn!$ $(1 \leq j \leq n)$ sont premiers entre eux deux à deux.

LEMME III.4.- Soient n et y tels que $1 \leq y \leq n$, et c défini par l'égalité $\prod_{j \leq y} (1 + jn!) = 1 + cn!$. Alors, $c \equiv k \pmod{1 + kn!}$, pour tout k tel que $1 \leq k \leq y$.

Démonstration du théorème III.1 : elle utilise en force les résultats du paragraphe II.

Soit $P(x_1,\ldots,x_p, y, z_1,\ldots,z_m)$ un polynôme à coefficients dans $\mathbb{Z}$ et soit $S(x_1,\ldots,x_p, y)$ la relation $\forall k \leq y \; \exists z_1 \ldots \exists z_m \; P(x_1,\ldots,x_p, k, z_1,\ldots,z_m) = 0$. Soit u le degré de P et s la somme des valeurs absolues de ses coefficients.

A) Nous montrons d'abord que $S(x_1,\ldots,x_p)$ est vraie si et seulement s'il existe des nombres f , n , c , $a_1,\ldots,a_m$ tels que les $5+m$ relations suivantes soient simultanément vérifiées :

(1) $n \geq s x_1^u \ldots x_p^u f^u y^u$ (2) $n \geq y$

(3) $n \geq f$ (4) $1 + cn! = \prod_{k \leq y} (1 + kn!)$

(5) $P(x_1,\ldots,x_p, c, a_1,\ldots,a_m) \equiv 0 \pmod{1 + cn!}$

(5+i) $\prod_{j \leq f} (a_i - j) \equiv 0 \pmod{1 + cn!}$.

Soient donnés my entiers $z_{i,k}$ tels que pour chaque $k \leq y$

$$P(x_1,\ldots,x_p, k, z_{1,k},\ldots, z_{m,k}) = 0 .$$

Soit $f = \sup\{z_{i,k} \mid i \leq m , k \leq y\}$, choisissons n de manière à satisfaire (1), (2), (3). Par (2) et d'après III.3 et le Théorème Chinois, il existe $a_1,\ldots,a_m$ tels que

pour chaque $i \leq m$, $a_i \equiv z_{i,k} \pmod{1 + kn!}$ pour $k \leq y$. Soit c défini par l'égalité (4). Par III.4, on a, pour chaque $k \leq y$:

$0 = P(x_1,\ldots,x_p , k , z_{1,k},\ldots,z_{m,k}) \equiv P(x_1,\ldots,x_p , c , a_1,\ldots,a_m) \pmod{1 + kn!}$,

d'où la congruence (5) en utilisant III.3. De même, comme $z_{i,k} \leq f$,

$$0 = \prod_{j \leq f} (z_{i,k} - j) \equiv \prod_{j \leq f} (a_i - j) \pmod{1 + kn!}$$

$$\equiv \prod_{j \leq f} (a_i - j) \pmod{1 + cn!} ,$$

d'où la relation (5 + i).

Inversement, soient donnés des nombres f , n , c , $a_1,\ldots,a_m$ qui vérifient les relations (1) à (5 + m). Pour chaque $k \leq y$, soit d_k un diviseur premier quelconque de $1 + kn!$ et soit $z_{i,k} = \text{Reste}\,(a_i,d_k)$. On a d'après (4), (5) et III.4 :

$$P(x_1,\ldots,x_p , k , z_{1,k},\ldots, z_{m,k}) \equiv 0 \pmod{d_k} .$$

Par (5 + i), on a $\prod_{j \leq f} (z_{i,k} - j) \equiv 0 \pmod{d_k}$. Or, d'après (3) et III.2, on a aussi $f \leq n < d_k$, donc $1 \leq z_{i,k} \leq f$ pour tout $i \leq m$ et tout $k \leq y$. Donc par (1) : $|P(x_1,\ldots,x_p , k , z_{1,k},\ldots,z_{m,k})| \leq n < d_k$, ce qui, joint à $P(x_1,\ldots,x_p , k , z_{1,k},\ldots,z_{m,k}) \equiv 0 \pmod{d_k}$, donne $P(x_1,\ldots,x_p , k , z_{1,k},\ldots,z_{m,k}) = 0$.

B) Pour montrer que $S(x_1,\ldots,x_p)$ est diophantienne, il suffit (par I.1) de montrer maintenant que chacune des relations (1) à (5 + m) est diophantienne. C'est clair pour (1), (2) et (3) en utilisant les exemples de I et I.2. Quant aux relations (4) à (5 + m), elles sont diophantiennes par II.10 et I.2.

C.Q.F.D.

IV. Les conséquences.

DÉFINITION.- Une relation est récursive si elle est récursivement énumérable et si sa négation est récursivement énumérable.

THÉORÈME IV.1 (Théorème fondamental de la théorie des fonctions récursives).- Il existe une relation récursivement énumérable à un argument qui n'est pas récursive.

DÉFINITION.- Une fonction est récursive si son graphe est récursivement énumérable.

On démontre facilement que le graphe d'une fonction récursive est une relation récursive, et que toute relation obtenue en substituant aux arguments d'une relation récursive des fonctions récursives est aussi récursive.

L'intérêt considérable de la notion de relation récursive provient en grande partie de son adéquation à la notion intuitive de relation effectivement décidable : une relation est dite effectivement décidable s'il existe un procédé général et "uniforme", défini une fois pour toutes, permettant de reconnaître pour chaque p-uplet $(x_1,\ldots,x_p)$, au moyen d'une suite finie et effectivement déterminée d'opérations effectivement réalisables, si $(x_1,\ldots,x_p)$ vérifie la relation ou non.

On peut affirmer (et il est facile de s'en convaincre au moyen du théorème III.1) que toute relation récursive est effectivement décidable. La réciproque de cette affirmation, qui est connue sous le nom de "Thèse de Church" et qui est largement admise, peut se justifier grâce aux remarques suivantes :

a) Tous les procédés effectifs de décision qui sont connus à l'heure actuelle se décomposent trivialement en un nombre restreint de composants élémentaires, qu'on peut mettre en parallèle avec des relations récursives élémentaires. Si l'on découvrait un jour une relation non récursive que l'on serait forcé de considérer comme effectivement décidable, la méthode de décision qui lui serait associée comporterait donc un procédé entièrement nouveau, et il est peu vraisemblable que ce fait se produise un jour.

b) La classe des relations récursives possède de bien meilleures propriétés mathématiques que les classes voisines, et ces propriétés sont précisément celles qu'on attendrait de la "classe" des relations effectivement décidables.

Une conséquence de a) est qu'il existe un processus uniforme, dépourvu d'astuces, ("filière de Church"), qui permet de transformer toute démonstration intuitive du caractère effectivement décidable d'une relation R en une démonstration mathématique de son caractère récursif. Par exemple, il est évident (crible d'Eratosthène) que la relation $P(x)$: " x est un nombre premier " est effectivement décidable. Donc $P(x)$ est une relation récursive, la démonstration de ce fait étant triviale.

Il est clair également que la relation $Q(x)$:

$$x \in \{1 , 2^2 , 3^{3^3} , \ldots , n^{n^{\cdot^{\cdot^{\cdot^{n}}}}} , \ldots\}$$

est effectivement décidable ; on démontre, toujours trivialement, bien que la démonstration soit plus longue, que la relation $Q(x)$ est récursive.

Toute relation récursive étant diophantienne, la richesse de la classe des relations diophantiennes est donc considérable. Cette richesse a pour conséquences des propriétés remarquables, que nous illustrons par deux exemples caractéristiques :

A) Conséquences de type positif.

THÉORÈME IV.2.- Tout sous-ensemble E récursivement énumérable de $\mathbb{N}^+$ (c'est-à-dire qui est tel que la relation $x \in E$ est récursivement énumérable) est l'ensemble des valeurs positives d'un certain polynôme à coefficients dans $\mathbb{Z}$.

En effet, puisque E est diophantien, il existe un polynôme P tel que

$x \in E$ si et seulement si $\exists\, x_1 \in \mathbb{N}^+ \ldots \exists\, x_p \in \mathbb{N}^+ \quad P(x_1,\ldots,x_p , x) = 0$

si et seulement si $\exists\, x_1 \in \mathbb{N}^+ \ldots \exists\, x_p \in \mathbb{N}^+ \exists\, y \in \mathbb{N}^+ \quad [x = (1 - P^2(x_1,\ldots,x_p,y))y]$.

Les exemples d'ensembles récursifs qui ont été vus plus haut fournissent le

COROLLAIRE IV.3.- Il existe un polynôme P_1 à coefficients dans $\mathbb{Z}$ dont l'ensemble des valeurs positives est l'ensemble des nombres premiers. Il existe un polynôme Q_1 à coefficients dans $\mathbb{Z}$ dont l'ensemble des valeurs positives est

$$\{1 , 2^2 , 3^{3^3} , \ldots , n^{n^{\cdot^{\cdot^{\cdot^{n}}}}} , \ldots\} .$$

Ce dernier ensemble étant très "rare" sans être fini ne peut être l'ensemble de toutes les valeurs d'un polynôme, ni a fortiori l'ensemble de toutes les valeurs d'un polynôme à coefficients ≥ 0 , obtenues pour des valeurs positives des variables.

B) Conséquences de type négatif. Le 10e Problème de Hilbert.

Soit $\mathbb{P}$ l'ensemble des polynômes (d'un nombre quelconque de variables) à coefficients dans $\mathbb{Z}$. Il est facile de trouver une numérotation de $\mathbb{P}$ (cf. [5]), c'est-à-dire une bijection f de $\mathbb{N}^+$ sur $\mathbb{P}$, qui possède les propriétés suivantes :

. Les opérations élémentaires sur les polynômes (addition, multiplication, substitution d'un élément de $\mathbb{N}^+$ à une variable donnée ...) se traduisent via f par des fonctions récursives sur $\mathbb{N}^+$.

. En particulier la fonction $\varphi(m,a)$ définie comme suit :

$f(\varphi(m,a))$ est le polynôme obtenu en remplaçant dans le polynôme $f(m)$ la variable x_1 par a

est récursive. Grâce à une telle bijection f , les problèmes d'effectivité qui se posent sur $\mathbb{P}$ peuvent recevoir un sens précis. Soit H la relation définie par :

$H(n)$ si et seulement si le polynôme $f(n)$ a des solutions dans $\mathbb{N}^+$.

Le 10e Problème de Hilbert peut alors s'énoncer ainsi :

La relation H est-elle récursive ?

Le théorème III.1 et le théorème fondamental IV.1 permettent de donner immédiatement une réponse négative à ce problème.

THÉORÈME IV.4.- La relation H n'est pas récursive.

Note ajoutée en août 1971 :

Les formules suivantes, qui conduisent à une démonstration simple du corollaire II.10 ne faisant pas appel à II.9, m'ont été communiquées par Madame Julia Robinson :

$$\binom{k}{n} = \text{Reste}\left(\left[\frac{(u+1)^n}{u^k} \right], u \right) \qquad \text{pour} \quad u > 2^n$$

$$\prod_{k=1}^{n} (a + bk) = \text{Reste}\left(\left(\binom{n}{x+n} \right) n!\, b^n, t \right)$$

pour $t > (a + bn)^n$ et $bx \equiv a \pmod{t}$.

BIBLIOGRAPHIE

[1] David HILBERT - Mathematische Probleme. Vortrag gehalten auf dem internationalen Mathematiker-Kongress zu Paris 1900. Traduction anglaise, Bull. Amer. Math. Soc., 8 (1901/1902), 437-479.

[2] Julia ROBINSON - Existential definability in aritmetic, Trans. A.M.S., vol. 72 (1952), 437-449.

[3] Martin DAVIS, Hilary PUTNAM and Julia ROBINSON - The decision problem for exponential diophantine equations, Annals of Math., vol. 74 (1961), 425-436.

[4] Iu. V. MATIASEVITCH - Enumerable sets are diophantine, Soviet Mathematics, Mar-Apr. 1970, vol. 11, number 2, p. 354.

[5] Daniel LACOMBE - La théorie des fonctions récursives et ses applications, Bull. Soc. Math. France, 88 (1960), 393-468.

[6] Hilary PUTNAM - An unsolvable problem in number theory, J. of Symb. Logic, t. 25 (1960), 220-232.

[7] Martin DAVIS - An explicit diophantine definition of the exponential function, (non publié).