Revue de Mathématiques Spéciales

L'ensemble $\mathscr{P}$ des nombres premiers est diophantien

par Michel Collet, I.A.-I.P.R. de Mathématiques, Lille,
avec la collaboration de L. G. Vidiani, professeur de Mathématiques spéciales,
au lycée Carnot de Dijon.

Introduction.

Le polynôme suivant :

$$(k+2)[1-([wz+h+j-q]^2+[(gk+2g+k+1).(h+j)+h-z]^2+[16(k+1)^3.(k+2)(n+1)^2+1-f^2]^2$$
$$+[2n+p+q+z-e]^2+[e^3.(e+2).(a+1)^2+1-o^2]^2+[(a^2-1)y^2+1-x^2]^2$$
$$+[16r^2y^4.(a^2-1)+1-u^2]^2+[((a+u^2.(u^2-a))^2-1).(n+4dy)^2+1-(x+cu)^2]^2$$
$$+[(a^2-1)l^2+1-m^2]^2+[ai+k+1-l-i]^2+[n+l+v-y]^2+[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$+[q+y(a-p-1)+s.(2ap+2a-p^2-2p-2)-x]^2+[z+pl(a-p)+t(2ap-p^2-1)-pm]^2)]$$

de degré 25, à 26 variables, construit par l'américain James P. Jones, en 1976, ne présente pas que l'intérêt d'utiliser les vingt-six lettres de notre alphabet ! L'ensemble de ses valeurs strictement positives, pour des valeurs entières positives ou nulles de chacune de ses variables est exactement l'ensemble $\mathscr{P}$ des nombres premiers.

Nous dirons que ce polynôme est *une représentation diophantienne de* $\mathscr{P}$, ou encore, que $\mathscr{P}$ *est diophantien.*

La construction d'un tel polynôme est relativement simple, et accessible à un bachelier, série C, du temps où l'on enseignait l'Arithmétique en classe Terminale. Tout lecteur mathématicien devrait éprouver un certain plaisir à suivre la démonstration et témoigner une vive admiration aux inventeurs de la procédure mise en œuvre pour l'obtention de ce résultat.

L'étude qui suit n'a pour but que de décrire chacune des étapes du raisonnement. Il s'agit simplement, et sans prétention, d'analyser, en français, deux articles publiés dans la revue : « *American Mathematical Monthly* »,

– Martin Davis, *Hilbert's tenth problem is unsolvable*, March 73, pp. 233-269 ;

– James P. Jones, *Diophantine Representation of the set of prime numbers*, June-July 76, 449-464.

Les points forts de la construction sont énoncés sous forme de théorèmes dans la quatrième partie. Le second paragraphe a pour but d'établir des propriétés des solutions de l'équation de Pell, seules celles utiles à cette étude sont signalées, et cette partie ne constitue en aucun cas une étude exhaustive de ces équations. Le paragraphe 3 a pour objet une application immédiate d'un résultat démontré au paragraphe précédent. En préliminaire, nous établirons une double inégalité qui sera utilisée pour démontrer le théorème P_1.

Important.

Dans cette étude, toutes les variables (de a à z) prennent leurs valeurs dans l'ensemble $\mathbb{N}$ des nombres entiers naturels.

§ 1. Une double inégalité.

Nous allons établir les résultats suivants :

I. – *Pour tous entiers k, n et p satisfaisant à*

$$1 \leqslant k \leqslant n \leqslant n^k < p,$$

nous avons

$$0 < \sum_{i=0}^{k} \binom{n}{i} p^i < p^{k+1}.$$

II. – En outre, si $(2k)^k \leqslant n$, alors

$$(R) \qquad k! < \frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i} < k! + 1.$$

Démonstration :

I. – Puisque $p > 0$, l'inégalité de gauche est triviale.

Pour tout i, $i \geqslant 0$, nous avons $\binom{n}{i} \leqslant n^i$ (égalité pour $i = 0$ ou 1) donc

$$\sum_{i=0}^{k} \binom{n}{i} p^i \leqslant \sum_{i=0}^{k} n^i p^i = \frac{(np)^{k+1} - 1}{np - 1}.$$

Mais, par hypothèse, $n^k < p$, soit $n^k \leqslant p - 1$, donc

$$n^{k+1} \leqslant n(p-1) \leqslant np - 1,$$

par suite,

$$(np)^{k+1} - 1 < (np)^{k+1} \leqslant p^{k+1}(np-1),$$

d'où la double inégalité annoncée.

II. – Montrons d'abord l'inégalité de gauche dans la relation (R).

Nous avons

$$\sum_{i=0}^{k} \binom{n}{i} p^i = \sum_{i=0}^{k-1} \binom{n}{i} p^i + \binom{n}{k} p^k.$$

Comme $n \geqslant 2k$, pour i variant de 0 à $k-1$, les coefficients binômiaux $\binom{n}{i}$ sont croissants et

$$\binom{n}{i} \leqslant \binom{n}{k-1}$$

pour $0 \leqslant i \leqslant k-1$ et $p^i \leqslant p^{k-1}$; nous en déduisons

$$\sum_{i=0}^{k} \binom{n}{i} p^i \leqslant k\binom{n}{k-1} p^{k-1} + \binom{n}{k} p^k.$$

Mais, $\binom{n}{i} \leqslant \frac{n^i}{i!}$, il vient alors

$$\sum_{i=0}^{k} \binom{n}{i} p^i \leqslant \frac{kn^{k-1}p^{k-1}}{(k-1)!} + \frac{n^k p^k}{k!}.$$

d'où

$$k!\left[\sum_{i=0}^{k} \binom{n}{i} p^i\right] \leqslant k^2 n^{k-1} p^{k-1} + n^k p^k$$
$$\leqslant kn^k p^{k-1} + n^k p^k < (k + n^k) p^k$$

et comme

$$(k + n^k) \leqslant (n+1)^k,$$

nous en déduisons l'inégalité de gauche.

Montrons à présent l'inégalité de droite dans la relation (R).

Il est clair que

$$\binom{n}{k} p^k < \sum_{i=0}^{k} \binom{n}{i} p^i,$$

puisque $k > 0$, donc

$$\frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i} < \frac{(n+1)^k}{\binom{n}{k}} = \frac{k!}{\frac{(n-k+1)\ \ldots\ n}{(n+1)^k}}$$
$$\leqslant \frac{k!}{\left(\frac{n+1-k}{n+1}\right)^k} = \frac{k!}{\left(1 - \frac{k}{n+1}\right)^k}.$$

Mais, $\frac{k}{n+1} < \frac{k}{2^k k^k} = \frac{1}{2^k k^{k-1}} < \frac{1}{k}$ donc

$$\left(1 - \frac{k}{n+1}\right)^k \geqslant \left(1 - \frac{k^2}{n+1}\right).$$

De même $\frac{k^2}{n+1} < \frac{1}{2}$ donc

$$\left(1 - \frac{k^2}{n+1}\right)^{-1} \leqslant 1 + \frac{2k^2}{n+1},$$

d'où

$$\frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i} \leqslant k!\left(1 + \frac{2k^2}{n+1}\right) = k! + \frac{2k^2(k!)}{n+1}$$

et, nous obtenons successivement

$$\frac{2k^2(k!)}{n+1} < \frac{2k^2 k^{k-1}}{2^k k^k} = \frac{k}{2^{k-1}} \leqslant 1,$$

d'où la relation (R).

Conséquences.

Pour $p = (n+1)^k$, posons

$$h + j = \sum_{i=0}^{k} \binom{n}{i} (n+1)^{ki},$$

il vient

$$k! < \frac{(n+1)^{k^2+k}}{h+j} < k! + 1.$$

Ce dernier résultat sera utilisé dans la démonstration du théorème P_1, au paragraphe 4.

§ 2. L'équation de Pell P_a.

Nous désignerons par P_a, l'équation diophantienne

$$P_a : \quad X^2 - (a^2 - 1)Y^2 = 1,$$

pour $a \geqslant 2$. Pour $a = 1$, l'équation P_1 ne présente guère d'intérêt.

Les suites de Lucas.

Pour $a \geqslant 2$, le nombre $\sqrt{a^2-1}$ est irrationnel, et pour tout entier n,

$$(a + \sqrt{a^2-1})^n = u_n + v_n\sqrt{a^2-1}$$

où $(u_n, v_n) \in \mathbb{N}^2$ et cette décomposition est unique.

Pour simplifier l'écriture, nous poserons, dans cette section,

$$A = \sqrt{a^2-1}$$

ainsi

$$u_n + Av_n = (a + A)^n.$$

Pour $n = 0$, $u_0 = 1$, $v_0 = 0$ et

$$u_0^2 - (a^2-1)v_0^2 = 1.$$

Pour $n = 1$, $u_1 = a$, $v_1 = 1$ et

$$u_1^2 - (a^2-1)v_1^2 = 1.$$

Admettons cette propriété jusqu'au rang p : pour $0 \leqslant q \leqslant p$,

$$u_q^2 - (a^2-1)v_q^2 = 1$$

et considérons

$$u_{p+1} + Av_{p+1} = (a+A)^p (a+A) = (u_p + Av_p)(a+A).$$

Il vient

$$u_{p+1} = au_p + (a^2 - 1)v_p$$
$$v_{p+1} = u_p + av_p,$$

d'où

$$u_{p+1}^2 - (a^2 - 1)v_{p+1}^2 = 1.$$

et donc pour $n \geqslant 0$, (u_n, v_n) est une solution de l'équation P_a.

Pour $n \geqslant 1$, nous avons :

$$(u_{n-1} + Av_{n-1})(a + A) = (u_n + Av_n)$$
$$(u_{n-1} + Av_{n-1}) = (u_n + Av_n)(a - A)$$

car $(a + A)(a - A) = 1$, soit

$$u_{n-1} = au_n - (a^2 - 1)v_n ;$$
$$v_{n-1} = -u_n + av_n$$

comme

$$u_{n+1} = au_n + (a^2 - 1)v_n ;$$
$$v_{n+1} = u_n + av_n$$
$$u_{n+1} = 2au_n - u_{n-1}$$

et $$v_{n+1} = 2av_n - v_{n-1},$$

d'où les suites de LUCAS :

$u_0 = 1$, $u_1 = a$, et $u_{n+2} = 2au_{n+1} - u_n$

$v_0 = 0$, $v_1 = 1$, et $v_{n+2} = 2av_{n+1} - v_n$.

Réciproquement, si (X, Y) est une solution de l'équation P_a, puisque $a \geqslant 2$,

$$(a + A) > 1$$

et il existe un unique entier n tel que

$$(a + A)^n \leqslant (X + AY) < (a + A)^{n+1},$$

soit

$$u_n + Av_n \leqslant X + AY < (u_n + Av_n)(a + A)$$

et

$$1 \leqslant (X + AY)(u_n - Av_n) < (a + A)$$

car

$$(u_n + Av_n)(u_n - Av_n) = 1.$$

Comme

$$(X + AY)(X - AY)(u_n - Av_n)(u_n + Av_n) = 1,$$

$(x, y) = (Xu_n - A^2Yv_n, Yu_n - Xv_n)$ est une solution de l'équation P_a et nous avons les inégalités

$$1 \leqslant x + Ay < a + A$$

soit

$$1 \leqslant \frac{1}{x - Ay} < \frac{1}{a - A};$$

$$0 < a - A < x - Ay \leqslant 1$$

soit

$$-1 \leqslant -x + Ay < -a + A$$
$$1 \leqslant x + Ay < a + A$$

comme $0 \leqslant 2Ay < A$ et donc $y = 0$, soit $X = u_n$ et $Y = v_n$.

Nous avons établi le théorème :

Théorème.

Les solutions de l'équation diophantienne P_a :

$$X^2 - (a^2 - 1)Y^2 = 1$$

sont engendrées par les suites de Lucas :

X : $u_0 = 1$, $u_1 = a$ et $u_{n+2} = 2au_{n+1} - u_n$

Y : $v_0 = 0$, $v_1 = 1$ et $v_{n+2} = 2av_{n+1} - v_n$.

Étude des suites de Lucas.

1° Les suites (u_n) et (v_n) sont strictement croissantes $(a \geqslant 2)$.

Considérons pour $a \geqslant 2$, les suites (w_n) définies par w_0, w_1 et

$$w_{n+2} = 2aw_{n+1} - w_n,$$

nous avons

$$w_{n+2} - w_{n+1} = (2a-1)w_{n+1} - w_n$$
$$> w_{n+1} - w_n > \ldots > w_1 - w_0$$

et donc les suites (u_n) et (v_n) sont strictement croissantes.

2° Pour tout n, $(2a - 1)^n \leqslant v_{n+1} \leqslant (2a)^n$.

Pour $n = 0$, $v_1 = 1$, $(2a - 1)^0 \leqslant v_1 \leqslant (2a)^0$.

Pour $n = 1$, $v_2 = 2a$, $(2a - 1)^1 < v_2 \leqslant (2a)^1$.

Admettons la propriété jusqu'au rang p : $0 \leqslant q \leqslant p$:

$$(2a - 1)^q \leqslant v_{q+1} \leqslant (2a)^q$$

et considérons

$$v_{p+2} = 2av_{p+1} - v_p$$

Puisque $v_{p+1} > v_p$,

$$v_{p+2} > (2a - 1)v_{p+1} > (2a - 1)^{p+1}$$

De même

$$v_{p+2} < 2av_{p+1} \leqslant (2a)^{p+1}.$$

Donc, pour $n \geqslant 0$,

$$(2a - 1)^n \leqslant v_{n+1} \leqslant (2a)^n.$$

Les inégalités sont strictes pour $n \geqslant 2$.

3° Pour tout n, $v_n \equiv n \bmod (a - 1)$.

Nous supposerons évidemment $a \geqslant 2$.

Pour $n = 0$ et $n = 1$ c'est évident. Admettons la propriété jusqu'au rang p :

$$0 \leqslant q \leqslant p : v_q \equiv q \mod (a - 1).$$

Pour $p \geqslant 1$, nous avons

$$v_{p+1} = 2av_p - v_{p-1} ;$$

mais $a \equiv 1$, $v_p \equiv p$ et $v_{p-1} \equiv p - 1 \bmod (a - 1)$, donc

$$v_{p+1} \equiv 2p - (p - 1) = p + 1 \mod (a - 1),$$

d'où la congruence pour tout n

$$v_n \equiv n \mod (a - 1)$$

4° Pour $a \geqslant 2$, $n + 1 + v_n \leqslant v_{n+1}$.
Pour $n = 0$, $1 + v_0 = 1 \leqslant v_1$.
Pour $n = 1$, $2 + v_1 = 3 \leqslant v_2 = 2a$.
Admettons la propriété jusqu'au rang p : $0 \leqslant q \leqslant p$,

$$q + 1 + v_q \leqslant v_{q+1}.$$

Pour $p \geqslant 0$, nous avons

$$v_{p+2} = 2av_{p+1} - v_p,$$

puisque $v_{p+1} > v_p$,

$$v_{p+2} = v_{p+1} + (2a - 1)v_{p+1} - v_p > v_{p+1} + (2a - 2)v_{p+1}$$

et comme $v_{p+1} \geqslant p + 1$ car la suite (v_n) est strictement croissante,

$$v_{p+2} > v_{p+1} + (2a-2)(p+1) \geqslant v_{p+1} + 2p + 2 \geqslant p + 2 + v_{p+1},$$

d'où l'inégalité, pour tout n,

$$n + 1 + v_n \leqslant v_{n+1}.$$

5° Pour tout entier C, $u_n \equiv C^n + (a - C)v_n$, mod $(2aC - C^2 - 1)$.
Pour $n = 0$ et $n = 1$ c'est évident.
Admettons la propriété jusqu'au rang p : pour $0 \leqslant q \leqslant p$,

$$u_q \equiv C^q + (a - C)v_q \mod (2aC - C^2 - 1)$$

et considérons

$$u_{p+1} - (a - C)v_{p+1} = 2au_p - u_{p-1} - (a - C)(2av_p - v_{p-1})$$

$$u_{p+1} - (a - C)v_{p+1} = 2a[u_p - (a - C)v_p] - [u_{p-1} - (a - C)v_{p-1}]$$

$$u_{p+1} - (a - C)v_{p+1} = 2aC^p - C^{p-1} \mod (2a - C^2 - 1)$$

Mais, $2aC^p - C^{p-1} = C^{p-1}(2aC - 1)$ et

$$(2aC - 1) \equiv C^2 \mod (2aC - C^2 - 1)$$

d'où, pour tout n

$$u_n \equiv C^n + (a - C)v_n \mod (2aC - C^2 - 1).$$

En outre si $0 < C^n < a$, pour $n = 0$, ou 1,

$$C^n + (a - C)v_n = u_n.$$

Pour $n \geqslant 2$, $v_n \geqslant 2a$ et

$$a - 1 < [A - (a - 1)]2a \leqslant [A - (a - 1)]v_n$$

où $A^2 = a^2 - 1$. Par suite

$$C^n + (a - C)v_n \leqslant (a - 1) + (a - 1)v_n < Av_n$$

et comme, $Av_n < u_n$, pour tout n,

$$u_n \geqslant C^n + (a - C)v_n.$$

Ce résultat sera rappelé sous forme de lemme au moment de son utilisation dans le paragraphe suivant.

§ 3. De l'équation diophantienne (S) :

$$Z^3(Z + 2)(N + 1)^2 + 1 = X^2, \quad Z \geqslant 2.$$

Nous pouvons toujours poser $Z = a - 1$, ce qui implique $a \geqslant 3$. L'équation (S) devient

$$(a - 1)^3(a + 1)(N + 1)^2 + 1 = X^2,$$

soit

$$(a^2 - 1)[(a - 1)(N + 1)]^2 + 1 = X^2,$$

et, en posant $Y = (a - 1)(N + 1)$,

$$X^2 - (a^2 - 1)Y^2 = 1.$$

Nous reconnaissons une équation de Pell dont les solutions sont données par les suites de Lucas :

$$X = u_j, \qquad Y = v_j, \qquad j \in \mathbb{N}.$$

Il existe donc un entier j tel que

$$v_j = Y = (a - 1)(N + 1).$$

Nous avons, de toute évidence

$$v_j \equiv 0 \mod (a - 1)$$

mais, les termes de la suite (v_j) satisfont à la congruence (propriété 3 des suites de Lucas) :

$$v_j \equiv j \mod (a - 1).$$

Par conséquent $(a - 1)$ divise j et $(a - 1) \leqslant j$.
La suite (v_j) étant croissante,

$$v_{a-1} \leqslant v_j = (a - 1)(N + 1);$$

mais $(2a - 1)^{a-2} \leqslant v_{a-1}$, soit

$$(2a - 1)^{a-2} \leqslant (a - 1)(N + 1).$$

En observant que

$$(2a-1)^{a-2} = (a-1+a)^{a-2} > (a-1)^{a-2} + (a-2)(a-1)$$

il vient

$$(a-1)^{a-2} + (a-2)(a-1) < (a-1)(N+1).$$

soit

$$(a - 1)^{a-3} + (a - 2) < N + 1$$

ou encore

$$(a - 1)^{a-3} + (a - 2) \leqslant N,$$

d'où

$$Z - 1 + Z^{Z-2} \leqslant N.$$

Conséquences.

Si $Z = 2k$ et $N = n$, $(k \geqslant 1)$ la relation

$$(2k)^3(2k + 2)(n + 1)^2 + 1 = f^2$$

implique

$$2k - 1 + (2k)^{2k-2} \leqslant n,$$

d'où

$$n \geqslant (2k)^k.$$

Nous verrons encore trois applications de cette inégalité.

Rappelons la cinquième propriété des suites de Lucas :

Lemme.

Soit l'équation de Pell

$$X^2 - (a^2 - 1)Y^2 = 1, \qquad a \geqslant 1,$$

$(u_n, v_n)_{n \in \mathbb{N}}$ *les solutions de cette équation. Pour tout entier* C, *nous avons*

$$u_n \equiv C^n + (a - C)v_n \mod (2aC - C^2 - 1)$$

et si $0 < C^n < a$, *alors*

$$0 < C^n + (a - C)v_n \leqslant u_n.$$

Applications : Soit $n \geqslant (2k)^k$ pour $k \geqslant 1$; posons

$$e = p + q + z + 2n$$

et

$$e^3(e + 2)(a + 1)^2 + 1 = o^2.$$

De l'étude de l'équation diophantienne (S), il résulte que

$$e - 1 + e^{e-2} \leqslant a,$$

soit

$$p + q + z + 2n - 1 + (p + q + z + 2n)^{p+q+z+2n-2} \leqslant a$$

et donc

$$(p + q + z + 2n)^{p+q+z+2n-2} < a$$

d'où $(n + 1)^k < a$;

$$(p + 1)^n < a \qquad \text{et} \qquad p^{k+1} < a.$$

Appliquons maintenant trois fois le lemme précédent

1° En substituant k à n et $(n + 1)$ à C :

$$u_k \equiv (n + 1)^k + (a - n - 1)v_k \mod [2a(n + 1) - (n + 1)^2 - 1]$$

et comme $(n + 1)^k < a$ alors

$$0 < u_k \leqslant (n + 1)^k + (a - n - 1)v_k.$$

2° En substituant $(p + 1)$ à C :

$$u_n \equiv (p + 1)^n + (a - p - 1)v_n \mod [2a(p + 1) - (p + 1)^2 - 1]$$

et comme $(p + 1)^n < a$ alors

$$0 < u_n \leqslant (p + 1)^n + (a - p - 1)v_n.$$

3° En substituant p à C et k à n :

$$u_k \equiv p^k + (a - p)v_k \mod (2ap - p^2 - 1)$$
$$pu_k \equiv p^{k+1} + p(a - p)v_k \mod (2ap - p^2 - 1)$$

et comme $p^{k+1} < a$ alors

$$0 < pu_k \leqslant p^{k+1} + p(a - p)v_k.$$

Nous allons en déduire les expressions de p, q et z.

Calcul de p : Si nous posons

$$u_k = p + (a - n - 1)v_k + b[2a(n + 1) - (n + 1)^2 - 1],$$

nous en déduisons

$$p \equiv (n + 1)^k \mod [2a(n + 1) - (n + 1)^2 - 1]$$

mais,

$$p < a < 2a(n + 1) - (n + 1)^2 - 1$$

et

$$(n + 1)^k < a$$

donc

$$p = (n + 1)^k.$$

Calcul de q : Si nous posons

$$u_n = q + (a - p - 1)v_n + s[2a(p + 1) - (p + 1)^2 - 1],$$

nous en déduisons :

$$q \equiv (p + 1)^n \mod [2a(p + 1) - (p + 1)^2 - 1]$$

mais,

$$q < a < 2a(p + 1) - (p + 1)^2 - 1$$

et

$$(p + 1)^n < a$$

donc

$$q = (p + 1)^n.$$

Calcul de z : Si nous posons

$$pu_k = z + p(a - p)v_k + t(2ap - p^2 - 1),$$

nous en déduisons

$$z = p^{k+1} \mod (2ap - p^2 - 1)$$

mais,

$$z < a < 2ap - p^2 - 1$$

et

$$p^{k+1} < a$$

donc

$$z = p^{k+1}.$$

C'est pour le théorème P_2 que ces résultats sont importants.

§ 4. Construction du polynôme de James P. Jones.

C'est à partir du théorème de Wilson, $k + 1$ est premier *si, et seulement si*, $k + 1$ divise $k ! + 1$ que nous donnerons une représentation diophantienne de l'ensemble $\mathscr{P}$ des nombres premiers.

Théorème P_1.

Soit k un entier, $k \geqslant 1$; $k + 1$ est premier si et seulement si il existe 6 entiers : f, g, h, j, n et w tels que

(A) $[(n+1)^k+1]^n = w(n+1)^{k^2+k}+h+j$

(B) $(n+1)^{k^2+k} = (gk+k+g)(h+j)+h$

(C) $(2k)^3(2k+2)(n+1)^2+1 = f^2.$

Démonstration :

— *Les conditions* (A), (B) *et* (C) *sont nécessaires.* Par hypothèse $k + 1$ est premier. D'après le théorème de Wilson, $k + 1$ divise $k ! + 1$, donc

il existe un entier g tel que

$$k! + 1 = (g + 1)(k + 1)$$

soit

$$k! = gk + k + g.$$

L'équation (C) se ramène à une équation de Pell (voir étude de l'équation diophantienne (S)), elle admet donc des solutions n, les équations (A) et (B) s'obtiennent par divisions euclidiennes.

Il est évidemment plus intéressant de montrer que :

– *Les conditions* (A), (B) *et* (C) *sont suffisantes.* La condition (C) étant satisfaite, nous pouvons trouver n tel que

$$n \geqslant (2k)^k,$$

d'après l'étude de l'équation diophantienne (S). Nous obtenons alors

$$(n + 1)^k + 1 \equiv 1 \mod (n + 1)$$

donc

$$[(n + 1)^k + 1]^n \equiv h + j \mod (n + 1)^{k^2+k}$$

et

$$0 < h + j < (n + 1)^{k^2+k}$$

et

$$h + j = \sum_{i=0}^{k} \binom{n}{i} (n + 1)^{ki}.$$

D'après la relation (B) :

$$gk+k+g \leqslant \frac{(n+1)^{k^2+k}}{h+j} \leqslant gk+k+g+1$$

mais, de l'inégalité fondamentale (R) :

$$k! < \frac{(n + 1)^{k^2+k}}{h + j} < k! + 1.$$

Comme $gk + k + g$ et $gk + k + g + 1$ sont deux entiers consécutifs

$$gk + k + g = k!$$

soit

$$k! + 1 = (g + 1)(k + 1).$$

Le théorème de Wilson permet de conclure.

Corollaire.

Soit k un entier, $k \geqslant 1$; $k + 1$ est premier si et seulement si il existe 9 entiers : f, g, h, j, n, p, q, w et z tels que

(1) $q = wz + h + j$
(2) $z = (gk + k + g)(h + j) + h$
(3) $(2k)^3(2k + 2)(n + 1)^2 + 1 = f^2$

(*a*) $p = (n + 1)^k$
(*b*) $q = (p + 1)^n$
(*c*) $z = p^{k+1}$

La démonstration de ce corollaire est immédiate.

Théorème P_2.

Soit k un entier, $k \geqslant 1$; $k + 1$ est premier si et seulement si il existe 19 entiers : a, b, e, f, g, h, j, l, m, n, o, p, q, s, t, w, x, y et z tels que

(1) $q = wz + h + j$
(2) $z = (gk + k + g)(h + j) + h$
(3) $(2k)^3(2k + 2)(n + 1)^2 + 1 = f^2$
(4) $e = p + q + z + 2n$
(5) $e^3(e + 2)(a + 1)^2 + 1 = o^2$
(6) $x^2 = (a^2 - 1)y^2 + 1$
(7′) $x = u_n$
(9) $m^2 = (a^2 - 1)l^2 + 1$
(10′) $l = v_k$
(12) $m = p + l(a - n - 1) + b[2a(n + 1) - (n + 1)^2 - 1]$
(13) $x = q + y(a - p - 1) + s[2a(p + 1) - (p + 1)^2 - 1]$
(14) $pm = z + pl(a - p) + t(2ap - p^2 - 1)$.

Démonstration :

– *Les 12 conditions précédentes sont nécessaires.* D'après le corollaire du théorème P_1, si $k + 1$ est premier, nous avons (1), (2) et (3) et nous connaissons les 9 entiers : f, g, h, j, n, p, q, w et z. e est obtenu par (4), (5) détermine a et o. La connaissance de n permet de déterminer x par (7′) et y par (6). De même, la connaissance de k permet de déterminer l par (10′) et m par (9). Enfin, b, s, t sont déterminés par (12), (13) et (14).

– *Les 12 conditions précédentes sont suffisantes.* D'après les calculs de p, q et z faits avant le théorème P_1 :

(4), (5), (9), (10′) et (12) impliquent (*a*) ;
(4), (5), (6), (7′) et (13) impliquent (*b*) ;
(4), (5), (9), (10′) et (14) impliquent (*c*).

et, (1), (2), (3), (*a*), (*b*) et (*c*) impliquent $k + 1$ premier, d'où le théorème P_2.

Il nous reste à modifier les conditions (7′) et (10′). Pour ce faire, nous aurons recours au résultat suivant qui caractérise la suite (v_n) solution en y de l'équation de Pell (6).

Nous démontrerons en annexe le lemme suivant :

Lemme.

Étant donné deux nombres entiers a et n, $1 \leqslant n$ et $2 \leqslant a$, $y = v_n$ si et seulement si il existe 5 entiers c, d, r, u et x tels que

(6) $x^2 = (a^2 - 1)y^2 + 1$
(7) $u^2 = 16(a^2 - 1)r^2y^4 + 1$
(8) $(x + cu)^2 = \{[a + u^2(u^2 - a)]^2 - 1\}(n + 4dy)^2 + 1$
(11′) $n \leqslant y$.

Ce résultat étant admis, nous en déduisons le

Théorème P_3.

Soit k un entier, $k \geqslant 1$, $k+1$ est premier si et seulement si, il existe 23 entiers : a, b, c, d, e, f, g, h, j, l, m, n, o, p, q, r, s, t, u, w, x, y et z tels que :

(1) $q = wz + h + j$

(2) $z = (gk + k + g)(h + j) + h$

(3) $(2k)^3(2k+2)(n+1)^2 + 1 = f^2$

(4) $e = p + q + z + 2n$

(5) $e^3(e+2)(a+1)^2 + 1 = o^2$

(6) $x^2 = (a^2-1)y^2 + 1$

(7) $u^2 = 16(a^2-1)r^2y^4 + 1$

(8) $(x+cu)^2 = \{[a+u^2(u^2-a)]^2 - 1\}(n+4dy)^2 + 1$

(9) $m^2 = (a^2-1)l^2 + 1$

(10′) $l = v_k$

(11′) $n \leqslant y$

(12) $m = p + l(a-n-1) + b[2a(n+1) - (n+1)^2 - 1]$

(13) $x = q + y(a-p-1) + s[2a(p+1) - (p+1)^2 - 1]$

(14) $pm = z + pl(a-p) + t(2ap - p^2 - 1)$.

Démonstration : Compte tenu du lemme précédent, il nous suffit de remarquer que les conditions (6), (7), (8) et (11′) sont équivalentes aux conditions (6) et (7′) du théorème P_2, les autres conditions étant inchangées.

Modifions pour terminer les conditions (10′) et (11′). L'équation (9) implique d'après (10′)

$$m = u_k \quad \text{et} \quad l = v_k.$$

Nous savons que

$$v_k \equiv k \mod (a-1)$$

et nous pouvons écrire

(10) $$l = k + i(a-1).$$

(v_n) est une suite croissante, donc $v_n \geqslant n$ soit $v_k \geqslant k$ et $i \geqslant 0$.

D'autre part, nous avons pour tout n,

$$n + v_{n-1} \leqslant v_n$$

comme $k < n$, $l \leqslant v_{n-1}$ et $n + l \leqslant y$ soit

(11) $$n + l + v = y.$$

qui implique (11′).

Inversement, si les conditions (9), (10) et (11) sont vérifiées, (9) et (11′) sont manifestement satisfaites.

D'après la condition (9), nous avons

$$m = u_{k'} \quad \text{et} \quad l = v_{k'}$$

comme d'après (11), $l < y$, alors

$$v_{k'} < v_n \quad \text{et} \quad k' < n.$$

D'après l'étude de l'équation diophantienne (S)

$$k < (a-1) \quad \text{et} \quad k' < (a-1)$$

et puisque $l \equiv k \mod (a-1)$ mais aussi $l \equiv k' \mod (a-1)$,

$$k = k' \quad \text{et} \quad l = v_{k'}$$

c'est la condition (10′).

Les conditions (1) à (14) constituent donc une condition nécessaire et suffisante pour que $k+1$ soit premier.

En substituant $k+1$ à k dans les conditions (2), (3) et (10) nous pouvons énoncer le théorème :

Théorème

Soit k un entier, $k \geqslant 0$; $k+2$ est un nombre premier si et seulement si il existe 25 entiers : a, b, …, j, l, …, x, y et z tels que

(1) $A = wz + h + j - q = 0$

(2) $B = (gk + 2g + k + 1)(h + j) + h - z = 0$

(3) $C = 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2 = 0$

(4) $D = 2n + p + q + z - e = 0$

(5) $E = e^3(e+2)(a+1)^2 + 1 - o^2 = 0$

(6) $F = x^2 - (a^2-1)y^2 - 1 = 0$

(7) $G = 16(a^2-1)r^2y^4 + 1 - u^2 = 0$

(8) $H = \{[a+u^2(u^2-a)]^2 - 1\}(n+4dy)^2 + 1 - (x+cu)^2 = 0$

(9) $I = m^2 - (a^2-1)l^2 - 1 = 0$

(10) $J = i(a-1) + k + 1 - l = 0$

(11) $K = n + l + v - y = 0$

(12) $L = p + l(a-n-1) + b[2a(n+1) - (n+1)^2 - 1] - m = 0$

(13) $M = q + y(a-p-1) + s[2a(p+1) - (p+1)^2 - 1] - x = 0$

(14) $N = z + pl(a-p) + t(2ap - p^2 - 1) - pm = 0.$

Cette condition peut s'écrire :

$$A^2 + B^2 + C^2 + D^2 + E^2 + F^2 + G^2 + H^2 + I^2 + J^2 + K^2 + L^2 + M^2 + N^2 = 0$$

ou encore

$$1 - \sum_{i=A}^{N} i^2 = 1,$$

et nous conclurons : le polynôme

$$P(a, b, \ldots, z) = (k+2)\left(l - \sum_{A}^{N} i^2\right)$$

de degré 25 à 26 variables, variant dans l'ensemble $\mathbb{N}$, est tel que l'ensemble de ses valeurs positives coïncide avec l'ensemble des nombres premiers.

ANNEXE

Compléments sur les solutions de l'équation de Pell.

Complément C_1

Soit les équations de Pell :

P_a : $X^2 - (a^2 - 1)Y^2 = 1$, (u_j, v_j) *ses solutions*
P_b : $X^2 - (b^2 - 1)Y^2 = 1$, (s_j, t_j) *ses solutions*

Si $b \equiv a \bmod u$, *alors pour tout entier* j, $s_j \equiv u_j \bmod u$.

Démonstration : Nous avons

$$s_0 = 1 \quad \text{et} \quad u_0 = 1 \quad \text{donc} \quad s_0 \equiv u_0 \mod u$$
$$s_1 = b \quad \text{et} \quad u_1 = a \quad \text{donc} \quad s_1 \equiv u_1 \mod u$$

Les relations de récurrence (suites de Lucas)

$$s_{p+2} = 2bs_{p+1} - s_p$$

et

$$u_{p+2} = 2au_{p+1} - u_p$$

conduisent immédiatement au résultat par récurrence sur p.

Complément C_2

Pour $0 < i \leqslant k$, *si* $u_j \equiv u_i \bmod u_k$ *alors :*

$$j \equiv \pm i \mod 4k.$$

Démonstration : Comme au paragraphe 2, nous avons :

$$u_{k\pm m} + Av_{k\pm m} = (u_k + Av_k)(u_m \pm Av_m),$$

d'où

$$u_{k\pm m} = u_k u_m + (a^2 - 1)v_k v_m$$

et

$$v_{k\pm m} = v_k u_m \pm u_k v_m$$

soit

- pour $m = k \pm i$,

$$u_{2k\pm i} = u_k u_{k\pm i} + (a^2 - 1)v_k v_{k\pm i} ;$$

- pour $m = i$,

$$v_{k\pm i} = v_k u_i \pm u_k v_i$$

et

$$u_{2k\pm i} = u_k u_{k\pm i} + (a^2 - 1)v_k(v_k u_i \pm u_k v_i)$$

donc

$$u_{2k\pm i} \equiv (a^2 - 1)v_k^2 u_i \mod u_k.$$

Comme, $(a^2 - 1)v_k^2 = u_k^2 - 1 = -1 \mod u_k$

$$u_{2k\pm i} \equiv -u_i \mod u_k.$$

Par conséquent

$$u_{4k\pm i} = u_{2k+(2k\pm i)} \equiv -u_{2k\pm i} \equiv u_i \mod u_k$$

et pour tout entier p, $p \geqslant 1$,

$$u_{4pk\pm i} \equiv u_i \mod u_k$$

Pour prouver le résultat C_2, il suffit donc de montrer que pour $j \leqslant 2k$, si $u_j \equiv u_i \bmod u_k$, alors $j = i$.

Remarquons alors que si $p + q = k$,

$$u_{k+p} = u_{2k-q}$$

et

$$u_{k+p} \equiv -u_q \bmod u_k.$$

Nous savons que la suite (u_n) est strictement croissante, et que pour tout n,

$$2u_{n-1} < u_n,$$

(exception pour $a = 2$ et $n = 1$), par conséquent, modulo u_k, les classes de $-u_{k-1}, -u_{k-2}, \ldots, -u_0, u_0, \ldots, u_k$ sont distinctes deux à deux, de même que les classes de $u_0, u_1, \ldots, u_{2k-1}, u_{2k}$ et donc, si $j \leqslant 2k$, alors $j = i$, d'où le résultat.

Complément C_3

Si v_i^2 *divise* v_k, *alors* v_i *divise* k.

Démonstration :

Scolie : v_i divise v_k *si et seulement si* i divise k.
Manifestement, pour $i \neq 0$, v_i divise v_i. Comme

$$v_{i(q+1)} = v_{i+qi} = v_i u_{qi} + u_i v_{qi},$$

un raisonnement par récurrence sur q montre que la condition est suffisante.

Inversement, si v_i divise v_k, posons

$$k = qi + r, \qquad 0 \leqslant r < i,$$

alors

$$v_k = u_r v_{qi} + u_{qi} v_r$$

Comme, v_i divise v_k et v_{qi}, v_i divise $u_{qi}v_r$, mais, u_{qi} et v_{qi} sont premiers entre eux, donc v_i et u_{qi} sont premiers entre eux (car v_i divise v_{qi}) et par conséquent, v_i divise v_r. Comme, $r < i$, $v_r < v_i$, d'où $v_r = 0$ et $r = 0$. Ce qui démontre la scolie.

Si v_i^2 divise v_k, en particulier v_i divise v_k et $k = qi$. Comme,

$$u_{qi} + Av_{qi} = (u_i + Av_i)^q$$

$$v_{qi} = \sum_{\substack{j=0 \\ j=2p+1}}^{q} \binom{q}{2p+1} u_i^{q-j} v_i^j (a^2 - 1)^p$$

$$v_k = v_{qi} \equiv \binom{q}{1} u_i^{q-1} v_i \mod v_i^2$$

$$v_k \equiv q u_i^{q-1} v_i \mod v_i^2$$

et

$$v_k \equiv 0 \mod v_i^2.$$

Or u_i et v_i sont premiers entre eux, par suite v_i divise q, donc v_i divise k.

Complément C_4.

$$v_{4nv_n} \text{ est divisible par } 4v_n^2.$$

En effet, il suffit de remarquer que

$$\binom{4v_n}{2p+1} \equiv 0 \mod 4.$$

Nous sommes maintenant en mesure de justifier le lemme utilisé dans la démonstration du théorème P_3.

Lemme

Étant donné deux nombres entiers a et n, $1 \leqslant n$ et $2 \leqslant a$, $y = v_n$ si et seulement si il existe cinq entiers c, d, r, u et x tels que

(6) $x^2 = (a^2 - 1)y^2 + 1$

(7) $u^2 = 16(a^2 - 1)r^2y^4 + 1$

(8) $(x + cu)^2 = \{[a + u^2(u^2 - a)]^2 - 1\}(n + 4dy)^2 + 1$

(11') $n \leqslant y$.

Démonstration :

• *a) La condition est nécessaire.*

Si $y = v_n$, la condition (11') est automatiquement satisfaite, et pour $x = u_n$, nous obtenons la condition (6).

Posons alors, $u = u_{4nv_n}$, d'après le complément C_4, v_{4nv_n} est divisible par $4v_n^2$, donc

$$v_{4nv_n} = 4rv_n^2,$$

d'où r, et nous obtenons (7).

Enfin, en posant $b = a + u^2(u^2 - a)$,

$$b \equiv a \mod u_{4nv_n},$$

et les solutions (s_j, t_j) de l'équation de Pell P_b sont telles que

$$s_j \equiv u_j \mod u_{4nv_n},$$

d'après le complément C_1 donc, pour $j = n$,

$$s_n = x_n + cu_{4nv_n},$$

d'où la valeur de c.

Mais, $u^2 \equiv 1 \mod 4v_n$ et donc $b - 1 \equiv 0 \mod 4v_n$. Comme,

$$t_n \equiv n \mod b - 1,$$
$$t_n \equiv n \mod 4v_n$$

et

$$t_n = n + 4dv_n$$

d'où d et la condition (8).

• *b) La condition est suffisante.*

Posons, avec des notations évidentes :

$$x = u_i, \quad y = v_i,$$
$$u = u_k, \quad 4rv_i^2 = v_k,$$
$$u_i + cu_k = s_j \quad \text{et} \quad n + 4dv_i = t_j.$$

Il suffit de montrer que $i = n$.

D'une part, si nous posons

$$b = a + u^2(u^2 - a),$$

nous avons

$$b \equiv a \mod u_k,$$

et d'après le complément C_1 :

$$s_j \equiv u_j \mod u_k$$

mais,

$$s_j = u_i + cu_k$$

donc

$$s_j \equiv u_i \mod u_k$$

et donc

$$u_j \equiv u_i \mod u_k$$

Comme v_i divise visiblement v_k, $v_i \leqslant v_k$ et $i \leqslant k$, d'après le complément C_2 :

$$j \equiv \pm i \mod 4k.$$

Comme v_i^2 divise v_k, d'après le complément C_3, v_i divise k et

$$j \equiv \pm i \mod 4v_i.$$

D'autre part, $t_j = n + 4dv_i$ donc

$$t_j \equiv n \mod 4v_i$$

et, comme dans la condition nécessaire

$$t_j \equiv j \mod 4v_i$$

soit

$$j \equiv n \mod 4v_i.$$

Puisque $0 < i \leqslant v_i$ et $n \leqslant v_i$, nous pouvons conclure :

$$i = n \quad \text{et} \quad y = v_n$$

ce qui achève la démonstration du lemme.

Bibliographie

[1] Bouvier, *Dictionnaire*, PUF 1979, page 358, 10e problème de Hilbert.

[2] Brette François le lionnais, *Les nombres remarquables*, Hermann 1983, page 146.

[3] Cuculière Roger, APM Bulletin 342, pages 31-40 : *Représentation diophantienne des nombres de Fibonacci.*

[4] Jones James P., *Diophantine representation of the set of prime numbers*, American Mathematical Monthly, June-July 1976, pp. 449-464.

[5] Martin, Davis, *Hilbert's tenth problem is unsolvable*, March 1973, p. 233-269.

[6] Walcschmidt, *Le monde*, 26 octobre 1977, page 19.