Mémoire de mathématiques de première année : Le 10ème problème de Hilbert est indécidable

Paul Fraux Louis Hemmer-Petitcolas

2017

Table des matières

1 Exposé du problème et définitions **2**
1.1 Ensembles diophantiens 2
1.2 Fonctions récursives 3

2 Caractère diophantien de l'exponentielle et premières conséquences **3**
2.1 L'exponentielle est diophantienne 3
2.2 Conséquences 6

3 Constructions intermédiaires et équivalence des fonctions diophantiennes et récursives **8**
3.1 Fonctions spéciales 8
3.2 Stabilité des ensembles diophantiens par les quantifications bornées 9
3.3 Équivalence entre fonctions diophantiennes et fonctions récursives 12

4 10ème problème de Hilbert : preuve et conséquences **13**
4.1 Ensemble diophantien universel 13
4.2 La diophantianité n'est pas le tout ! 15
4.3 Le 10ème problème de Hilbert 15
4.4 Conséquence étonnante de la preuve du 10ème problème de Hilbert 16

5 Définition existentielle **16**
5.1 Cas de $\mathbb{Z}$ et $\mathbb{N}$ 16
5.2 Cas général 17

6 Cas des anneaux intègres de caractéristique nulle **18**

7 Cas de certains corps de fractions rationnelles **20**

Conclusion **24**

A Les 24 lemmes **25**

B Les sommes de carrés **26**

C Les courbes elliptiques **27**

Lors du congrès international des mathématiciens de 1900, le mathématicien David Hilbert propose une liste de 24 problèmes qui résistent alors encore aux mathématiciens, et qui devront, d'après lui, marquer le XXème siècle.
Nous allons dans ce document nous intéresser au dixième problème de Hilbert, défini ainsi par Hilbert :

> **10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.**
> Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt : man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Ce qui se traduit par :

> **10. De la possibilité de résoudre une équation de Diophante.**
> On donne une équation de Diophante à un nombre quelconque d'inconnues et à coefficients entiers rationnels : On demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombre entiers rationnels.

Nous allons montrer dans la première partie, à partir de l'article [1], que la réponse à ce problème est non. Puis nous étendrons ce résultat, à d'autres structures que $\mathbb{Z}$, grâce à [2].

Dans tout ce document, quand un nombre n'est pas défini a priori, il est par défaut entier positif non-nul.

1 Exposé du problème et définitions

Cette partie va permettre de formaliser la notion d'équations diophantiennes, et la notion de "nombre fini d'opérations" (qu'on appelle aujourd'hui *algorithme*).

1.1 Ensembles diophantiens

Définition. Soit p un entier non-nul. Soit $E \subset (\mathbb{N}^*)^p$. On dit que E est diophantien si et seulement si il existe $m \in \mathbb{N}$, il existe P un polynôme à $p+m$ indéterminées, à coefficients entiers, tel que :

$$E = \{(x_1, ..., x_p) \in (\mathbb{N}^*)^p \,|\exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m \,, P(x_1, ..., x_p, y_1, ..., y_m) = 0\}.$$

1.1.1 Exemples

- L'ensemble des nombres entiers non-nuls qui ne sont pas une puissance de 2 est diophantien. En effet, avec $P(X, Y, Z) = Y(2Z + 1) - X$,

$$E = \{x \in \mathbb{N}^* | \exists (y, z) \in (\mathbb{N}^*)^2 \,, P(x, y, z) = 0\}.$$

- Le graphe de la relation d'ordre stricte est diophantien. En effet, le polynôme $P(X, Y, Z) = x + z - y$ convient.
- Le graphe de la relation de divisibilité est diophantien. En effet, le polynôme $P(X, Y, Z) = xz - y$ convient.

1.1.2 Premières propriétés

Proposition 1.1. Soient E et F deux ensembles diophantiens, alors $E \cap F$ et $E \cup F$ sont diophantiens.

dem Soient P_E et P_F des polynômes définissant respectivement les ensembles E et F.
- Le polynôme $P_E^2 + P_F^2$ définit l'ensemble $E \cap F$.
- Le polynôme $P_E P_F$ définit l'ensemble $E \cup F$.

•

Exemple L'ensemble $E = \{(x, y, z) \in (\mathbb{N}^*)^3 \,, (x|y) \wedge (x < z)\}$ est diophantien, car $P(X, Y, Z, U, V) = (Y - XU)^2 + (Z - (X + V))^2$ le définit.

1.1.3 Fonctions diophantiennes

Définition. Soit $p \in \mathbb{N}^*$, soit $f : (\mathbb{N}^*)^p \to \mathbb{N}^*$. On dit que f est diophantienne si et seulement si l'ensemble $\{(x_1, ..., x_p, y) \in (\mathbb{N}^*)^{p+1} \,|y = f(x_1, ..., x_p)\}$ est diophantien, id est, son graphe est diophantien.

1.2 Fonctions récursives

Définition. L'ensemble des fonctions récursives, noté $\mathfrak{Rec}$, est la plus petite classe de fonctions contenant :

- Pour tout $p \in \mathbb{N}^*$, la *fonction constante* $\begin{array}{rccc} c_p & : & (\mathbb{N}^*)^p & \to & \mathbb{N}^* \\ & & x & \mapsto & 1 \end{array}$.
- La *fonction successeur* : $\begin{array}{rccc} s & : & \mathbb{N}^* & \to & \mathbb{N}^* \\ & & x & \mapsto & x+1 \end{array}$.
- Les *projections* : pour tout $n \in \mathbb{N}^*$, pour tout $i \in [\![1, n]\!]$, $\begin{array}{rccc} p_i^n & : & \mathbb{N}^n & \to & \mathbb{N} \\ & & (x_1, ..., x_n) & \mapsto & x_i \end{array}$.

et stable par :

- *composition*, i.e. : pour tout $f \in \mathfrak{Rec}_m$, pour tout $(g_1, ..., g_m) \in \mathfrak{Rec}_n^m$, on a :

$$\begin{array}{rccc} h & : & (\mathbb{N}^*)^n & \to & \mathbb{N}^* \\ & & (x_1, ..., x_n) & \mapsto & f(g_1(x_1, ..., x_n), ..., g_m(x_1, ..., x_n)) \end{array} \in \mathfrak{Rec}.$$

- *récurrence primitive*, i.e., pour tout $f \in \mathfrak{Rec}_n$, pour tout $g \in \mathfrak{Rec}_{n+2}$, la fonction h, définie par

$$\left\{ \begin{array}{rcl} h(x_1, ..., x_n, 1) & = & f(x_1, ..., x_n) \\ h(x_1, ..., x_n, t+1) & = & g(t, h(x_1, ..., x_n), x_1, ..., x_n) \end{array} \right. ,$$

  est récursive.
- *minimisation*, i.e., pour tout $(f, g) \in \mathfrak{Rec}_{n+1}^2$, si on suppose que pour tout $(x_1, ..., x_n) \in (\mathbb{N}^*)^n$, l'ensemble $\{y \in \mathbb{N}^* | f(x_1, ..., x_n, y) = g(x_1, ..., x_n, y)\}$ est non-vide, alors la fonction

$$\begin{array}{rccc} h & : & (\mathbb{N}^*)^n & \to & \mathbb{N} \\ & & (x_1, ..., x_n) & \mapsto & \min\{y \in \mathbb{N}^* | f(x_1, ..., x_n, y) = g(x_1, ..., x_n, y)\} \end{array} \in \mathfrak{Rec}.$$

Remarque. On montrera par la suite que l'ensemble des fonctions récursives correspond aux fonctions diophantiennes.

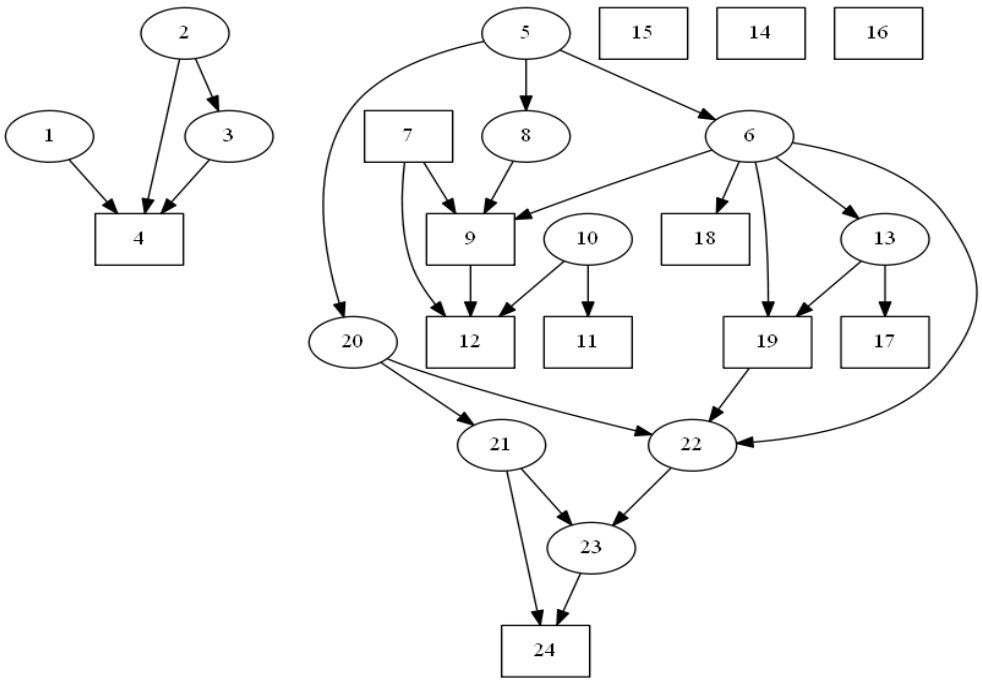
Remarque. La notion de fonctions récursives formalise la notion d'algorithmes (ou de nombre fini d'opérations).

2 Caractère diophantien de l'exponentielle et premières conséquences

2.1 L'exponentielle est diophantienne

On appelle exponentielle la fonction $\begin{array}{rccc} f & : & (\mathbb{N}^*)^2 & \to & \mathbb{N}^* \\ & & (n, k) & \mapsto & n^k \end{array}$. C'est le caractère diophantien de cette fonction qui a longuement résisté aux mathématiciens qui se sont intéressés au 10ème problème de Hilbert, et qui permet de faire fonctionner toute la preuve. Et c'est finalement Matiiassevitch, en 1970, qui le démontra, au travers d'un autre résultat que nous énoncerons plus loin.

Pour montrer que l'exponentielle est diophantienne, l'article [1] établit d'abord 24 lemmes, qui se trouvent en annexe A, sur les solutions des équations de Pell (voir ci-dessous). Les liens entre ces lemmes sont illustrés par le schéma ci-dessous :



où la flèche $\rightarrow$ signifie "sert à la démonstration de". Les lemmes entourés par un rectangle sont ceux qui servent à montrer les théorèmes 2 et 3 (voir plus loin).

2.1.1 Solution des équations de Pell

Soit $a \in \mathbb{N}^*$. On pose $(P_a) : x^2 - (a^2-1)y^2 = 1$. Cette équation est appelée équation de Pell. On note $E_a = \{(x,y) \in \mathbb{N}^2 | x^2 - (a^2-1)y^2 = 1\}$, et $F_a = \{(x,y) \in \mathbb{Z}^2 | x^2 - (a^2-1)y^2 = 1\}$.
Les lemmes 1 à 4 de l'annexe A se résument en le théorème suivant :

Théorème 1. On définit, pour tout $n \in \mathbb{N}$, $x_n(a), y_n(a)$ (aussi notés x_n et y_n si il n'y a pas d'ambuiguïtés) les uniques entiers tels que $x_n(a) + y_n(a)\sqrt{d} = (a+\sqrt{d})^n$. Alors :

$$E_a = \{(x_n(a), y_n(a)) | n \in \mathbb{N}\}.$$

dem Le plus simple est de passer par les 4 premiers lemmes de l'annexe A :

A.1 Soit $(x,y) \in F_a$. On a pas : $1 < x + y\sqrt{d} < a + \sqrt{d}$.
Supposons par l'absurde que l'inégalité soit vraie. Puisque (x,y) est une solution à l'équation de Pell, on a $(x+y\sqrt{d})(x-y\sqrt{d}) = 1$. Alors, $1 < \dfrac{1}{x-y\sqrt{d}} < \dfrac{1}{a-\sqrt{d}}$, donc $-1 < -x + y\sqrt{d} < -a + \sqrt{d}$, et en additionnant avec la première inégalité, on obtient $0 < 2y\sqrt{d} < 2\sqrt{d}$, donc $0 < y < 1$. Or, $y \in \mathbb{N}$, donc c'est absurde.

A.2 Soit $(x,y) \in F_a$ et $(x',y') \in F_a$, on définit $(x'',y'') \in \mathbb{Z}^2$ les uniques entiers tels que $x'' + y''\sqrt{d} = (x+y\sqrt{d})(x'+y'\sqrt{d})$. Alors $(x'',y'') \in F_a$.
En effet, on a alors $x'' - y''\sqrt{d} = (x-y\sqrt{d})(x'-y'\sqrt{d})$, et on a en même temps $x''+y''\sqrt{d} = \dfrac{1}{x-y\sqrt{d}} \cdot \dfrac{1}{x'-y'\sqrt{d}}$. Donc, en multipliant $(x'')^2 - d(y'')^2 = 1$.

A.3 Pour tout $n \in \mathbb{N}$, $(x_n(a), y_n(a)) \in E_a$. Cela se montre facilement par récurrence en utilisant A.2, et en remarquant que $(a,1) \in E_a$.

A.4 Ce lemme-ci correspond au théorème. Soit $(x,y) \in E_a$. On a $a+\sqrt{d} > 1$, donc la suite $\left((a+\sqrt{d})^n\right)_{n\in\mathbb{N}}$ diverge vers $+\infty$, donc il existe $n \in \mathbb{N}$ tel que

$$(a+\sqrt{d})^n \leq x + y\sqrt{d} < (a+\sqrt{d})^{n+1},$$

car ou bien $x = 1$ et alors $(x,y) = (x_0(a), y_0(a))$, ou bien $x > 1$ et donc $x + y\sqrt{d} > 1 = x_0(a) + y_0(a)$.
Si il y a égalité dans l'inégalité de gauche, alors on a fini. Sinon, en réécrivant :

$$x_n(a) + y_n(a)\sqrt{d} < x + y\sqrt{d} < (x_n(a) + y_n(a)\sqrt{d})(a+\sqrt{d}).$$

Or, $(x_n(a) + y_n(a)\sqrt{d})(x_n(a) - y_n(a)\sqrt{d}) = 1$, donc, $x_n(a) - y_n(a)\sqrt{d} > 0$, donc en multipliant par ce dernier la dernière inégalité, on obtient :

$$1 < (x + y\sqrt{d})((x_n(a) - y_n(a)\sqrt{d})) < a + \sqrt{d}.$$

Or, par A.1 et A.2, ceci est impossible.

•

2.1.2 Condition nécessaire et suffisante pour vérifier $x = x_k(a)$

Théorème 2. On définit le système d'équations suivantes :

$$\begin{aligned}
x^2 - (a^2-1)y^2 &= 1, && (1)\\
u^2 - (a^2-1)v^2 &= 1, && (2)\\
s^2 - (b^2-1)t^2 &= 1, && (3)\\
v &= ry^2, && (4)\\
b &= 1 + 4py = a + qu, && (5)\\
s &= x + cu, && (6)\\
t &= k + 4(d-1)y, && (7)\\
y &= k + e - 1. && (8)
\end{aligned}$$

Soit $a \in \mathbb{N}^*$, soit $k \in \mathbb{N}^*$, soit $x \in \mathbb{N}^*$. Alors : $x = x_k(a)$ si et seulement si le système d'équations $(1) - (8)$ admet des solutions pour les inconnues restantes, id est, il existe $(y, u, v, s, t, b, r, p, q, c, d, e) \in (\mathbb{N}^*)^{12}$ vérifiant $(1) - (8)$.

dem Nous n'allons pas en faire la démonstration complète, voir [1] pour celle-ci.
Par les trois premières équations, on a l'existence de $(i, n, j) \in (\mathbb{N}^*)^3$ tel que : $x = x_i(a)$, $y = y_i(a)$, $u = x_n(a)$, $v = y_n(a)$, $s = x_j(b)$, $t = y_j(b)$. Puis, en combinant les lemmes et les équations, on obtient les trois congruences suivantes :

1. $j \equiv \pm i \pmod{4y_i(a)}$,
2. $y_j(b) \equiv j \pmod{4y_i(a)}$,
3. $y_j(b) \equiv k \pmod{4y_i(a)}$.

Ce qui nous permet d'obtenir $k \equiv \pm i\ [4y_i(a)]$. Puis l'équation (8) donne $k \leq y_i(a)$ et le lemme 2.18 donne $i \leq y_i(a)$. Donc $i = k$, et on a obtenu ce qu'on voulait.
La réciproque se devine après avoir fait le sens direct, car celui-ci permet de comprendre le sens de chaque inconnue.

•

2.1.3 Condition nécessaire et suffisante pour vérifier $m = n^k$

Théorème 3. On adjoint au système d'équations $(1) - (8)$ les équations suivantes :

$$\begin{aligned}
(x - y(a-n) - m)^2 &= (f-1)^2(2an - n^2 - 1)^2, && (9)\\
m + g &= 2an - n^2 - 1, && (10)\\
w = n + h &= k + l, && (11)\\
a^2 - (w^2-1)(w-1)^2z^2 &= 1. && (12)
\end{aligned}$$

Soit $(n, m, k) \in (\mathbb{N}^*)^3$. Alors : $n = m^k$ si et seulement si le système d'équations $(1) - (12)$ admet des solutions pour les inconnues restantes.
Ceci nous donne le caractère diophantien de l'exponentielle.

dem Encore une fois, nous n'en donnons pas la démonstration complète, voir [1] pour celle-ci.
On montre d'abord, grâce au théorème précédent, que $x = x_k(a)$ et $y = y_k(a)$. Puis, nous obtenons par (9) et le lemme A.17 que $m \equiv n^k \ \left[\mathrm{mod}\ 2an - n^2 - 1\right]$.
Puis on montre que $m < 2an - n^2 - 1$ en remarquant par (12) que $a = x_j(w)$, et $(w-1)z = y_j(w)$, donc par le lemme $A.14$:

$$j \equiv 0 \ \left[\mathrm{mod}\ w - 1\right].$$

Donc $j \leq w - 1$ car $j > 0$. Et alors, par l'équation (11) et le lemme A.19, on obtient :

$$a \geq w^{w-1} > n^k.$$

Et donc, par (10), $m < 2an - n^2 - 1$. Et pour obtenir $n^k < 2an - n^2 - 1$, on utilise le fait que si $\alpha > \beta^\gamma$ (avec $\alpha, \beta, \gamma > 0$), alors $2\alpha\beta - \beta^2 - 1 > \beta^\gamma$, ce qui se démontre en étudiant la fonction $\beta \mapsto 2\alpha\beta - \beta^2 - 1$. La réciproque s'effectue en détaillant le sens direct pour comprendre le rôle de chaque inconnue (par exemple, h et l ne serve qu'à dire que $w > n$ et $w > k$).

•

2.2 Conséquences

Le but de cette partie est de montrer le caractère diophantien des fonctions suivantes :

$$\begin{array}{rcccl} f & : & (\mathbb{N}^*)^2 & \to & \mathbb{N}^* \\ & & (n,k) & \mapsto & \binom{n}{k} \end{array}, \qquad \begin{array}{rcccl} g & : & \mathbb{N}^* & \to & \mathbb{N}^* \\ & & n & \mapsto & n! \end{array},$$

$$\begin{array}{rcccl} h & : & (\mathbb{N}^*)^3 & \to & \mathbb{N}^* \\ & & (a,b,k) & \mapsto & \displaystyle\prod_{j=1}^{k}(a+bj) \end{array}.$$

On note, pour tout $x \in \mathbb{R}^+$, $\lfloor x \rfloor$ la partie entière de x, i.e., l'unique entier vérifiant :$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

2.2.1 La binomiale est diophantienne

Lemme 2.1. Pour tout $k \in [\![1, n]\!]$, et $u > 2^n$, on a :

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}.$$

Et donc :

$$\left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \equiv \binom{n}{k} \ [u].$$

dem

$$\frac{(u+1)^n}{u^k} = \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = S + R$$

avec $S = \displaystyle\sum_{i=k}^{n} \binom{n}{i} u^{i-k}$, et $R = \displaystyle\sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$. Alors S est entier, et montrons que $R < 1$:

$$\begin{array}{rcl} R & < & u^{-1} \displaystyle\sum_{i=0}^{k-1} \binom{n}{i} \\ & < & u^{-1} \displaystyle\sum_{i=0}^{n} \binom{n}{i} \\ & = & u^{-1} 2^n \\ & < & 1 \end{array}$$

•

Théorème 4. f est diophantienne.

dem On a :

$$z = f(n,k) \Leftrightarrow \exists u,v,w, \begin{cases} v &= 2^n \\ u &> v \\ w &= \left\lfloor \frac{(u+1)^n}{u^k} \right\rfloor \\ z &\equiv w \ [\text{mod } u] \\ z &< u \end{cases} .$$

•

2.2.2 La factorielle est diophantienne

Lemme 2.2. On montre de même que si : $r > (2x)^{x+1}$, alors

$$x! = \left\lfloor r^x \Big/ \binom{r}{x} \right\rfloor$$

Théorème 5. g est diophantienne.

dem C'est évident avec le lemme précédent.

•

2.2.3 Le "produit" est diophantien

Lemme 2.3. Soit $(a,b,q,M) \in (\mathbb{N}^*)^4$ tel que $bq \equiv a \ [M]$. Alors :

$$\forall k \in \mathbb{N}^*, \prod_{j=1}^{k}(a+bj) \equiv b^y y! \binom{q+y}{y} \ [M].$$

dem

$$\begin{aligned} b^k k! \binom{q+k}{k} &= b^k \prod_{i=1}^{k}(q+i) \\ &= \prod_{i=1}^{k}(bq+bi) \\ &\equiv \prod_{i=1}^{k}(a+ib) \ [M] \end{aligned}$$

•

Théorème 6. h est diophantienne.

dem Dans le précédent lemme, on prend $M = b(a+bk)^k+1$. Alors, $\text{pgcd}(M,b) = 1$, donc b est inversible pour la congruence modulo M, donc il existe $q \in \mathbb{N}^*$ tel que $bq \equiv a \ [M]$. De plus, $M > \prod_{i=1}^{k}(a+bi)$. Donc, $\prod_{i=1}^{k}(a+bi)$ est l'unique entier tel que $n < M$ et $n \equiv b^y y! \binom{q+y}{y} \ [M]$. Ce qui s'écrit :

$$z = \prod_{i=1}^{k}(a+ib) \Leftrightarrow \exists M,p,q,r,s,t,u,v,w,x, \begin{cases} r &= a+by \\ s &= r^y \\ M &= bs+1 \\ bq &= a+Mt \\ u &= b^y \\ v &= y! \\ z &< M \\ w &= q+y \\ x &= \binom{w}{y} \\ z+Mp &= uvx \end{cases} .$$

•

3 Constructions intermédiaires et équivalence des fonctions diophantiennes et récursives

3.1 Fonctions spéciales

3.1.1 Fonction paire

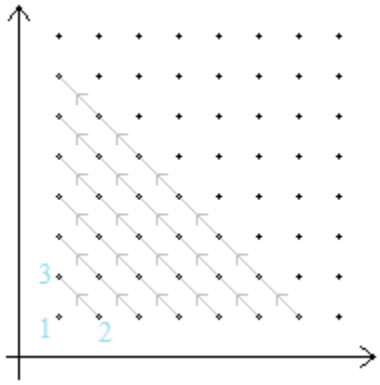
Définition. On définit : $L : \mathbb{N}^* \to \mathbb{N}^*$, $R : \mathbb{N}^* \to \mathbb{N}^*$, $P : (\mathbb{N}^*)^2 \to \mathbb{N}^*$ par :

$$x = L(z) \Leftrightarrow \exists y, 2z = (x+y-2)(x+y-1) + 2y,$$

$$y = R(z) \Leftrightarrow \exists x, 2z = (x+y-2)(x+y-1) + 2y,$$

$$z = P(x,y) \Leftrightarrow 2z = (x+y-2)(x+y-1) + 2y.$$

Remarque. En fait, P correspond à la bijection diagonale de $(\mathbb{N}^*)^2$ dans $\mathbb{N}^*$



Et L et R correpondent "aux bijections réciproques" de P : L étant la partie gauche (*Left* en anglais), et R étant la partie droite (*Right* en anglais). Donc ces fonctions sont bien définies.

Remarque. Par définition même, ces fonctions sont diophantiennes.

Propriété. Pour tout $z \in \mathbb{N}^*$, $L(z) \leq z$ et $R(z) \leq z$.

3.1.2 Fonction de codage des suites finies

Proposition 3.1. Il existe une fonction $S : (\mathbb{N}^*)^2 \to \mathbb{N}^*$ diophantienne telle que :
- $\forall (i,u) \in (\mathbb{N}^*)^2, S(i,u) \leq u$
- $\forall (a_1, ..., a_n) \in (\mathbb{N}^*)^n, \exists u \in \mathbb{N}^*, \forall i \in [\![1,n]\!], S(i,u) = a_i$

Remarque. Cette fonction code toutes les suites finies. (et correspond en fait à la fonction β de Gödel)

dem On définit $S(i,u)$ comme le reste de la division euclidienne de $L(u)$ par $1+iR(u)$. S est diophantienne. Car $w = S(i,u)$ ssi il existe x, y, z, v tels que :

$$\begin{cases} 2u & = & (x+y-2)(x+y-1)+2y) \\ x & = & w + z(1+iy)) \\ 1+iy & = & w+v-1 \end{cases}.$$

La première équation permet de dire $x = L(u)$ et $y = R(u)$. Et cette propriété est bien diophantienne en tant que conjonction de propriétés diophantiennes.
On voit que $S(i,u) \leq L(u) \leq u$.

Puis, soit $(a_1, ..., a_n) \in (\mathbb{N}^*)^n$, on choisit y plus grand que tous les a_i et tel que $n! \mid y$. Alors les $1 + iy$ pour $i \in [\![1, n]\!]$ sont deux à deux premiers entre eux. En effet, si $d|1 + iy$ et $d|1 + jy$, alors $d|j(1 + iy) - i(1 + jy) = j - i$. Donc, $d \leq n$, et ainsi, $d|y$, par conséquent $d|1$, d'où $d = 1$.
Donc, d'après le théorème chinois, il existe $x \in \mathbb{N}^*$, tel que

$$\forall i \in [\![1, n]\!],\ x \equiv a_i[1 + iy].$$

On pose alors $u = P(x, y)$ (la fonction paire), et alors $x = L(u)$ et $y = R(u)$, et comme $a_i < y = R(u) < 1 + iR(u)$, on a $a_i = S(i, u)$.

•

3.2 Stabilité des ensembles diophantiens par les quantifications bornées

On a vu précédemment que les fonctions $n \mapsto n!$, $(n, k) \mapsto \binom{n}{k}$ et $(a, b, k) \mapsto \prod_{i=1}^{k}(a + ib)$ sont diophantiennes.

Notation On écrit la quantification existentielle bornée « $(\exists y)_{\leq x}, ...$ », qui signifie « $\exists y, (y \leq x) \wedge ...$ ».
On écrit aussi la quantification universelle bornée, « $(\forall y)_{\leq x}, ...$ », qui signifie « $\forall y, (y \leq x) \Rightarrow ...$ »

Le but de cette partie est de montrer le théorème suivant :

Théorème 7. Si P est un polynôme à coefficients entiers, les ensembles S et R définis ci-dessous sont diophantiens.

$$R = \left\{(y, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1} \mid (\exists z)_{\leq y}, \exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m, P(y, z, x_1, ..., x_p, y_1, ..., y_m) = 0\right\},$$

$$S = \left\{(y, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1} \mid (\forall z)_{\leq y}, \exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m, P(y, z, x_1, ..., x_p, y_1, ..., y_m) = 0\right\}.$$

Remarque. Le fait que R est diophantien est trivial, car

$$(y, x_1, ..., x_p) \in R \Leftrightarrow (\exists z, y_1, ..., y_m)(z \leq y \wedge P(y, z, x_1, ..., x_p, y_m) = 0),$$

et que cette condition est évidemment diophantienne (cf. premiers exemples). C'est la preuve de la deuxième partie du théorème qui va demander un peu plus d'ingéniosité et de doigté.

Lemme 3.2. Avec les mêmes notations qu'avant, pour tout $(x_1, ..., x_p) \in (\mathbb{N}^*)^p$:

$$(\forall k)_{\leq y}, (\exists y_1, ..., y_m), P(y, k, x_1, ..., x_p, y_1, .., y_m) = 0$$

$$\Leftrightarrow$$

$$\exists u, (\forall k)_{\leq y}, (\exists y_1, ..., y_m)_{\leq u}, P(y, k, x_1, ..., x_p, y_1, .., y_m) = 0.$$

dem La réciproque de l'équivalence est clairement vraie. Occupons nous du sens direct.
Supposons que $(\forall k)_{\leq y}, (\exists y_1, ..., y_m), P(y, k, x_1, ..., x_p, y_1, .., y_m) = 0$, alors, pour chaque $k \in [\![1, y]\!]$, il existe des nombres $y_1^{(k)}, ..., y_m^{(k)}$ tels que :

$$P(y, k, x_1, ..., x_p, y_1^{(k)}, .., y_m^{(k)}) = 0.$$

En posant $u = \max\left\{y_j^{(k)} | (j, k) \in [\![1, m]\!] \times [\![1, y]\!]\right\}$, on a l'implication voulue.

•

Lemme 3.3. Soit $Q(y, u, x_1, ..., x_n)$ un polynôme avec les propriétés suivantes :

1. Pour tout $(y, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1}$, $Q(y, u, x_1, ..., x_n) > u$.
2. Pour tout $(u, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1}$, $Q(y, u, x_1, ..., x_n) > y$.
3. Pour tout $y \in \mathbb{N}^*$, $k \in [\![1, y]\!]$, $(u, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1}$, et pour tout $(y_1, ..., y_m) \in [\![1, u]\!]^m$,

$$|P(y, k, x_1, ..., x_p, y_1, ..., y_m)| \leq Q(y, u, x_1, ..., x_p).$$

Alors, pour tout $(y, u, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+2}$, on a l'équivalence entre les propositions suivantes :

1. $(\forall k)_{\leq y}, (\exists y_1, ..., y_m)_{\leq u}, P(y, k, x_1, ..., x_p, y_1, .., y_m) = 0$
2. Il existe $(c, t, a_1, ..., a_m) \in (\mathbb{N}^*)^{m+2}$,

$$\begin{cases} 1 + ct & = & \prod_{k=1}^{y}(1 + kt) \\ t & = & Q(y, u, x_1, ..., x_p)! \\ \forall i \in [\![1, m]\!], \quad 1 + ct & | & \prod_{j=1}^{u}(a_i - j) \\ P(y, c, x_1, ..., x_p, a_1, ..., a_m) & \equiv & 0 \ [\text{mod } (1 + ct)] \end{cases}.$$

Remarque. Le point numéro 2, malgré sa complexité apparente, est sans quantification bornée, ce qui le rend intéressant pour démontrer le théorème.

dem

– Prouvons $2 \Rightarrow 1$.

Pour chaque $k \in [\![1, y]\!]$, soit p_k un facteur premier de $1 + kt$. Soit, pour tout $(i, k) \in [\![1, m]\!] \times [\![1, y]\!]$, $y_i^{(k)}$ le reste de la division euclidienne de a_i par p_k. On va démontrer les deux points suivants pour tout i, k :

a) $1 \leq y_i^{(k)} \leq u$.

b) $P(y, k, x_1, ..., x_p, y_1^{(k)}, ..., y_m^{(k)}) = 0$.

Pour démontrer (a), on fixe d'abord $(i, k) \in [\![1, m]\!] \times [\![1, y]\!]$. Puis, on a $p_k | 1 + kt | 1 + ct | \prod_{j=1}^{u}(a_i - j)$.

Comme p_k est premier, il existe $j \in [\![1, u]\!]$, tel que $p_k | a_i - j$. Alors,

$$j \equiv a_i \equiv y_i^{(k)} \ [\text{mod } p_k].$$

On montre maintenant que $p_k > u$. En effet, en posant $t = Q(y, u, x_1, ..., x_p)!$, alors tout diviseur premier p de $1 + kt$ est tel que $p > Q(y, u, x_1, ..., x_p)!$, en particulier pour p_k (sinon, $p|t$, donc $p|1$). Or, d'après l'hypothèse (1) sur le polynôme Q, on sait que $Q(y, u, x_1, ..., x_p) > u$, donc $p_k > u$.
Comme $y_i^{(k)}$, est un reste division euclidienne par p_k, $y_i^{(k)} < p_k$. Donc $y_i^{(k)} = j \in [\![1, u]\!]$.

Montrons maintenant (b). Fixons $k \in [\![1, y]\!]$. On remarque :

$$1 + ct \equiv 1 + kt \equiv 0 \ [\text{mod } p_k].$$

Donc, $k + kct \equiv c + kct \ [\text{mod } p_k]$, i.e., $k \equiv c \ [\text{mod } p_k]$. Et comme par définition $y_i^{(k)} \equiv a_i \ [\text{mod } p_k]$, on a :

$$\begin{aligned} P(y, k, x_1, ..., x_p, y_1^{(k)}, ..., y_m^{(k)}) &\equiv P(y, k, x_1, ..., x_p, a_1, ..., a_m) \ [\text{mod } p_k] \\ &\equiv 0 \ [\text{mod } p_k]. \end{aligned}$$

Et comme on a de plus, par l'hypothèse (3) sur le polynôme Q, $\left|P(y, k, x_1, ..., x_p, y_1^{(k)}, ..., y_m^{(k)})\right| \leq Q(y, u, x_1, ..., x_p)$, et comme a on a montré précédemment que $Q(y, u, x_1, ..., x_p) < p_k$. On a donc le point (b).

– Montrons (1) $\Rightarrow$ (2). Soit, pour tout $k \in [\![1, y]\!]$, $(y_1^{(k)}, ..., y_m^{(k)}) \in [\![1, u]\!]^m$, tel que :

$$P(y, k, x_1, ..., x_p, y_1^{(k)}, ..., y_m^{(k)}) = 0$$

(qui existe par hypothèse).

On pose $t = Q(y, u, x_1, ..., x_p)!$, comme $\prod_{k=1}^{y}(1 + kt) \equiv 1 \ [\text{mod } t]$, il existe $c \in \mathbb{N}^*$:

$$1 + ct = \prod_{k=1}^{y}(1 + kt) \ .$$

On prend $(k, l) \in [\![1, y]\!]^2$ avec $k \neq l$, alors on a $\text{pcgd}(1 + kt, 1 + lt) = 1$, car si p est un diviseur commun à $1 + kt$ et $1 + lt$, alors $p|(l - k)$, donc $p < y$. Mais puisque $Q(y, u, x_1, ..., x_p) > y$, $p|t$, donc $p = 1$.

D'où, d'après le théorème chinois, pour tout $i \in [\![1, m]\!]$, il existe $a_i \in \mathbb{N}$, tel que, pour tout $k \in [\![1, y]\!]$

$$a_i \equiv y_i^{(k)} \ [\text{mod } 1 + kt] \, .$$

Par définition de c, pour tout $k \in [\![1, y]\!]$, $k \equiv c \ [\text{mod } 1 + kt]$, donc :

$$\begin{aligned} P(y, c, x_1, ..., x_p, a_1, ..., a_m) &\equiv P(y, k, x_1, ..., x_p, y_1^{(k)}, ..., y_m^{(k)}) \ [\text{mod } 1 + kt] \\ &\equiv 0 \ [\text{mod } 1 + kt]. \end{aligned}$$

Et comme les nombres $1 + kt$ sont deux à deux premiers entre eux, et comme chacun divise $P(y, c, x_1, ..., x_p, a_1, ..., a_m)$, leur produit le divise encore, donc :

$$P(y, c, x_1, ..., x_p, a_1, ..., a_m) \equiv 0 \ [\text{mod } 1 + ct] \, .$$

Or, par définition des a_i, (qui nous dit que $a_i \equiv y_i^{(k)} \ [\text{mod } 1 + kt]$), on a, pour tout $i \in [\![1, m]\!]$,

$$1 + kt \Big| a_i - y_i^{(k)} \ .$$

Et on a alors, pour tout $i \in [\![1, m]\!]$, (comme $1 \leq y_i^{(k)} \leq u$), on a :

$$1 + kt \left| \prod_{j=1}^{u}(a_i - j) \right. .$$

Puisque les $1 + kt$ sont encore premiers entre eux deux à deux, on a :

$$1 + ct \left| \prod_{j=1}^{u}(a_i - j) \right. .$$

Ce qui conclut.

•

Nous sommes maintenant en mesure de montrer le théorème 1.

dem
On écrit

$$P(y,k,x_1,...,x_p,y_1,...,y_n)=\sum_{r=1}^{N} t_r \ ,$$

avec t_r un monôme de la forme :

$$t_r = c\cdot y^a k^b x_1^{q_1}...x_p^{q_p} y_1^{s_1}...y_n^{s_n} \ ,$$

avec $c\in\mathbb{Z}$. Maintenant, on pose $u_r=|c|\cdot y^{a+b}x_1^{q_1}...x_p^{q_p}u^{s_1+...+s_n}$, et on pose :

$$Q(y,u,x_1,...,x_p)=u+y+\sum_{r=1}^{N} u_r \ .$$

Donc P et Q vérifient les hypothèses du lemme 3.3. Donc :

$$(\forall k)_{\leq y}\,, \exists y_1,...,y_m, P(y,k,x_1,...,x_p,y_1,...,y_n)=0$$

équivaut à :

$$\exists u,c,t,a_1,...,a_m, \begin{cases} 1+ct & = & \prod_{k=1}^{y}(1+kt) \\ t & = & Q(y,u,x_1,...,x_p)! \\ \forall i\in[\![1,m]\!],\ \ 1+ct & \mid & \prod_{j=1}^{u}(a_i-j) \\ P(y,c,x_1,...,x_p,a_1,...,a_m) & \equiv & 0\ [\mathrm{mod}\ (1+ct)] \end{cases} ,$$

qui équivaut à l'existence de $u,c,t,a_1,...,a_m,e,f,g_1,...,g_m,h_1,...,h_m$ des entiers strictement positifs tels que :

$$\begin{cases} e & = & 1+ct \\ e & = & \prod_{k=1}^{y}(1+kt) \\ f & = & Q(y,u,x_1,...,x_p) \\ t & = & f! \\ \forall i\in[\![1,m]\!],\ \ g_i & = & a_i-u-1 \\ \forall i\in[\![1,m]\!],\ \ h_i & = & \prod_{k=1}^{u}(g_i+k) \\ \forall i\in[\![1,m]\!],\ \ e & \mid & h_i \\ l & = & P(y,c,x_1,...,x_p,a_1,...,a_m) \\ e & \mid & l \end{cases} .$$

•

3.3 Équivalence entre fonctions diophantiennes et fonctions récursives

Théorème 8. Une fonction est récursive si et seulement si elle est diophantienne.

Notation On note $\mathfrak{Rec}$ l'ensemble des fonctions récursives, et exceptionnellement, on note $\mathfrak{Dioph}$ les fonctions diophantiennes.

Remarque. C'est ce résultat que Matiiassevitch parvint à démontrer en 1970, et qui utilise le caractère diophantien de l'exponentielle.

Rappel Il existe une fonction $S:(\mathbb{N}^*)^2\to\mathbb{N}^*$ qui est diophantienne et récursive, telle que :
- Pour tout $u\in\mathbb{N}^*$, pour tout $i\in\mathbb{N}^*$, $S(i,u)\leq u$
- Pour tout $(a_1,...,a_n)\in(\mathbb{N}^*)^n$, il existe $u\in\mathbb{N}^*$, tel que pour tout $i\in[\![1,n]\!]$, $S(i,u)=a_i$

dem

– Montrons d'abord $\mathfrak{Dioph} \subset \mathfrak{Rec}$. D'abord, $(x,y) \mapsto x+y$, $(x,y) \mapsto x \cdot y$, et pour tout $k \in \mathbb{N}^*$, $x \mapsto k$ sont diophantiennes. Donc, tout polynôme à coefficients entiers strictement positifs est récursif.
Soit $f \in \mathfrak{Dioph}$, alors il existe un polynôme H à coefficients entiers qui définit f, et on écrit

$$H = P - Q,$$

avec P et Q des polynômes à coefficients entiers strictement positifs, alors on a, pour tout $(y, x_1, ..., x_p) \in (\mathbb{N}^*)^{p+1}$,

$$\begin{aligned} y = f(x_1,...,x_p) &\Leftrightarrow \exists (t_1,...,t_m) \in (\mathbb{N}^*)^m, H(x_1,...,x_p,y,t_1,...,t_m) = 0, \text{ par définition} \\ &\Leftrightarrow \exists (t_1,...,t_m) \in (\mathbb{N}^*)^m, P(x_1,...,x_p,y,t_1,...,t_m) = Q(x_1,...,x_p,y,t_1,...,t_m). \end{aligned}$$

On a alors, pour tout $(x_1,...,x_p) \in (\mathbb{N}^*)^p$,

$$f(x_1,...,x_p) = S(1, \min\{u \in \mathbb{N}^* \,|P(x_1,..,x_p,S(1,u),...,S(m+1,u)) = Q(x_1,..,x_p,S(1,u),...,S(m+1,u))\}).$$

Et comme P, Q, S, sont récursifs, par composition et minimisation, f est récursive.

– Montrons désormais l'inclusion inverse : $\mathfrak{Rec} \subset \mathfrak{Dioph}$. Pour ce faire, nous allons montrer que les fonctions diophantiennes vérifient les propriétés définissant la classe des fonctions récursives (cf. la définition des fonctions récursives).

- Les fonctions $x \mapsto 1$, $x \mapsto x+1$ et $(x_1,...,x_p) \mapsto x_i$ sont trivialement diophantiennes.
- *Composition* : Soit $f \in \mathfrak{Dioph}_m$, soit $(g_1,...,g_m) \in \mathfrak{Dioph}_n$, soit h définie par :

$$\begin{array}{rccc} h & : & (\mathbb{N}^*)^n & \to & \mathbb{N}^* \\ & & (x_1,...,x_n) & \mapsto & f(g_1(x_1,...,x_n),...,g_m(x_1,...,x_n)) \end{array} \in \mathfrak{Rec}.$$

Alors h est aussi diophantienne. En effet, pour tout $(y, x_1, ..., x_n) \in (\mathbb{N}^*)^{n+1}$:

$$y = h(x_1,...,x_n) \Leftrightarrow \exists t_1,...,t_m, ((\forall i \in [\![1,m]\!], t_i = g_i(x_1,...,x_n)) \wedge (y = f(t_1,...,t_m))).$$

- *Récurrence primitive* : Soit $f \in \mathfrak{Dioph}_n$, soit $g \in \mathfrak{Dioph}_{n+2}$, soit h définie par :

$$\left\{ \begin{array}{rcl} h(x_1,...,x_n,1) & = & f(x_1,...,x_n) \\ h(x_1,...,x_n,t+1) & = & g(t,h(x_1,...,x_n),x_1,...,x_n) \end{array} \right. .$$

Alors, en utilisant la fonction de codage des suites finies (pour coder $(h(x_1,...,x_n,i))_{i \in [\![1,z]\!]}$), on a :

$$y = h(x_1,...,x_n,z) \Leftrightarrow \exists u, \left\{ \begin{array}{c} \exists v, (v = S(1,u) \wedge v = f(x_1,...,x_n)) \\ (\forall t)_{\leq z-1}, \exists v, ((v = S(t+1,u)) \wedge g(t,S(t,u),x_1,...,x_n)) \\ y = S(z,u) \end{array} \right. .$$

Donc, en utilisant la quantification bornée, h est diophantienne.

- *Minimisation* Soit $(f,g) \in \mathfrak{Dioph}^2_{n+1}$, si on suppose que pour tout $(x_1,...,x_n) \in (\mathbb{N}^*)^n$, l'ensemble $\{y \in \mathbb{N}^* | f(x_1,...,x_n,y) = g(x_1,...,x_n,y)\}$ est non-vide, alors on définit la fonction h par :

$$\begin{array}{rccc} h & : & (\mathbb{N}^*)^n & \to & \mathbb{N} \\ & & (x_1,...,x_n) & \mapsto & \min\{y \in \mathbb{N}^* | f(x_1,...,x_n,y) = g(x_1,...,x_n,y)\} \end{array} \in \mathfrak{Rec}.$$

Alors on a :

$$y = h(x_1,...,x_n) \Leftrightarrow \left\{ \begin{array}{c} \exists z, ((z = f(x_1,...,x_n,y)) \wedge (z = g(x_1,...,x_n,y))) \\ (\forall t)_{\leq y-1}, \exists u,v, (u = f(x_1,...,x_n,t) \wedge v = g(x_1,...,x_n,t) \wedge (u < v \text{ ou } v < u)) \end{array} \right. .$$

•

4 10ème problème de Hilbert : preuve et conséquences

4.1 Ensemble diophantien universel

Nous allons donner une énumération explicite de tous les ensembles diophantiens inclus dans $\mathbb{N}$ (qui sont évidemment en quantité dénombrable)
Pour cela, commençons par donner une énumération des polynômes à coefficients entiers positifs.

4.1.1 Enumeration des polynômes à coefficients entiers

On fixe $\mathcal{A} = \{X_0, X_1, ...\}$ un alphabet dénombrable de variables. L'énumération est la suite de polynômes $(P_n)_{n\in\mathbb{N}}$ définie par :

$$\begin{aligned} P_1 &= 1 \\ P_{3i-1} &= X_{i-1} \\ P_{3i} &= P_{L(i)} + P_{R(i)} \\ P_{3i+1} &= P_{L(i)} \cdot P_{R(i)} \end{aligned}$$

(car tout polynôme à coefficients entiers positifs peut être obtenue à partir de 1 et des variables de $\mathcal{A}$ par additions et multiplications successives)

Pour tout $i \in \mathbb{N}$, quand on écrira $P_i(X_0, ..., X_n)$, cela signifiera que n est assez grand pour contenir toutes les variables de P_i. Bien sûr, P_i ne dépendra pas de toutes ces variables.

4.1.2 Enumération des ensembles diophantiens

On pose, pour tout $n \in \mathbb{N}^*$:

$$D_n = \left\{ x_0 \in \mathbb{N}^* \,\middle|\, \exists (x_1, ..., x_n) \in (\mathbb{N}^*)^n \,, P_{L(n)}(x_0, x_1, ..., x_n) = P_{R(n)}(x_0, x_1, ..., x_n) \right\}.$$

Théorème 9. $(D_n)_{n\in\mathbb{N}^*}$ constitue une énumération des ensembles diophantiens inclus dans $\mathbb{N}$.

dem

D'abord, $P_{L(n)}$ et $P_{R(n)}$ ne dépendent clairement pas d'autres variables que X_0 jusqu'à X_n. Puis, soit un ensemble diophantien $E \subset \mathbb{N}$, défini par le polynôme P_E à coefficients entiers. Alors on peut trouver Q et R des polynômes à coefficients entiers positifs tels que $P_E = Q - R$. Il existe alors des entiers positifs r et q tels que $Q = P_q$ et $R = P_r$. Et alors, en posant $n = P(q, r)$ (la fonction paire, défini en 3.1.1).
Et alors, $E = D_n$.

•

4.1.3 Théorème de l'ensemble universel

Théorème 10. (De l'ensemble universel) L'ensemble $\{(n, x) | x \in D_n\}$ est diophantien.

dem On utilise encore une fois la fonction de codage des suites finies S. Montrons que

$$x \in D_n \Leftrightarrow \exists u \in \mathbb{N}^*, \begin{cases} S(1,u) &= 1 \\ S(2,u) &= x \\ (\forall i)_{\leq n}\,,\ S(3i,u) &= S(L(i),u) + S(R(i),u) \\ (\forall i)_{\leq n}\,,\ S(3i+1,u) &= S(L(i),u) \cdot S(R(i),u) \\ S(L(n),u) &= S(R(n),u) \end{cases}.$$

Et comme la partie droite de l'équivalence est clairement diophantienne, une fois que l'on aura montré cela, on aura fini la démonstration.
Soit $x \in D_n$. Par définition, il existe $(t_1, ..., t_n) \in (\mathbb{N}^*)^n$, $P_{L(n)}(x, t_1, ..., t_n) = P_{R(n)}(x, t_1, ..., t_n)$. Par définition de S, il existe $u \in \mathbb{N}^*$, tel que :

$$\forall j \in [\![1, 3n+2]\!], S(j, u) = P_j(x, t_1, ..., t_n).$$

En particulier, d'après le choix de l'énumération, $S(2, u) = x$ et pour tout $i \in [\![2, n+1]\!]$, $S(3i-1, u) = t_{i-1}$, D'où le sens direct.
Réciproquement, supposons qu'il existe $u \in \mathbb{N}^*$ vérifiant les bonnes hypothèses. Posons, pour tout $i \in [\![1, n]\!]$, $t_i = S(3i+2, u)$, alors par construction des P_i, on a nécessairement :

$$\forall j \in [\![1, 3n+2]\!], S(j, u) = P_j(x, t_1, ..., t_n).$$

Et comme $S(L(n), u) = S(R(n), u)$, on a nécessairement :

$$P_{L(n)}(x, t_1, ..., t_n) = P_{R(n)}(x, t_1, ..., t_n).$$

C'est-à-dire que : $x \in D_n$

•

4.2 La diophantianité n'est pas le tout !

Théorème 11. L'ensemble $V = \{n \in \mathbb{N}^* | n \notin D_n\}$ n'est pas diophantien.

dem Il s'agit en fait d'un argument de diagonale de Cantor.
Supposons par l'absurde que V est diophantien. Alors il existe $i \in \mathbb{N}^*$ tel que $V = D_i$. Et alors,
- Si $i \in V$, alors $i \notin D_i$, donc $i \notin V$.
- Si $i \notin V$, alors $i \in D_i$, donc $i \in V$.

Absurde.

•

Théorème 12. La fonction $g : (\mathbb{N}^*)^2 \mapsto \mathbb{N}^*$ définie par

$$g(n, x) = \begin{cases} 1 & \text{si} \quad x \notin D_n \\ 2 & \text{si} \quad x \in D_n \end{cases}$$

n'est pas récursive.

dem Si elle était récursive, elle serait diophantienne (d'après le théorème 8), et alors il existerait P un polynôme à coefficients entiers définissant g, id est,

$$y = g(n, x) \Leftrightarrow \exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m, P(n, x, y, y_1, ..., y_m) = 0.$$

Mais alors $V = \{x | \exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m, P(x, x, 1, y_1, ..., y_m) = 0\}$ serait diophantien, ce qui contredit le théorème 11.

•

4.3 Le 10ème problème de Hilbert

Théorème 13. Le 10ème problème de Hilbert dans $\mathbb{N}$ n'a pas de solutions.

dem Formellement, cela signifie qu'il n'existe pas de fonctions récursives $f : \mathbb{N}^* \mapsto \mathbb{N}^*$ tel que pour tout $n \in \mathbb{N}^*$, $f(n)$ soit 1 si $P_{L(n)} - P_{R(n)}$ admet une racine entière, et 0 sinon.
Supposons par l'aburde qu'il existe une telle fonction récursive. En utilisant le théorème 10, il existe P à coefficients entiers tel que :

$$x \in D_n \Leftrightarrow \exists z_1, ..., z_k, P(n, x, z_1, ..., z_k) = 0.$$

Alors pour n et x fixés, cette fonction peut calculer si

$$P(n, x, z_1, ..., z_k) = 0$$

admet des solutions, id est, si oui ou non $x \in D_n$. Cet algorithme peut alors être utilisé pour calculer $g(n, x)$. Ce qui est impossible.

•

4.4 Conséquence étonnante de la preuve du 10ème problème de Hilbert

Pour arriver au 10ème problème de Hilbert, nous avons du passer par de nombreux théorèmes, qui ont eux-mêmes des corollaires intéressants, nous avons choisi d'en exposer un ici, mais il y en a bien d'autres.

Définition. Pour un ensemble diophantien donné $E \subset \mathbb{N}$, on appelle dimension de E (noté $\dim E$), le plus petit entier $n \in \mathbb{N}$, tel qu'il existe un polynôme à coefficients entiers, à $n+1$ variables, définissant E.

Théorème 14. Il existe un entier m, tel que pour tout $E \subset \mathbb{N}$ ensemble diophantien, $\dim E \leq m$.

Remarque. On a même récemment montré, que $m \leq 14$!

dem Par le théorème de l'ensemble universel (théorème 10), il existe un polynôme P définissant l'ensemble universel. Donc,

$$\forall n \in \mathbb{N}^*, D_n = \{x \in \mathbb{N}^* | \exists (y_1, ..., y_m) \in (\mathbb{N}^*)^m, P(x, n, y_1, ..., y_m) = 0\}.$$

Donc $\dim D_n \leq m$. Donc, comme $(D_n)_{n\in\mathbb{N}}$ est une énumération des ensembles diophantiens, on a le résultat.

•

Exemple surprenant On note, pour tout $q \in \mathbb{N}^*$, $S_q = \{x \in \mathbb{N}^* | \exists (y_1, ..., y_q) \in (\mathbb{N}^*)^q, x = (y_1+1)...(y_q+1)\}$ (autrement dit, l'ensemble des entiers possédant au moins q facteurs premiers). Une conséquence du théorème 14 est que les S_q sont définissables avec moins de q paramètres pour q assez grand !

5 Définition existentielle

5.1 Cas de $\mathbb{Z}$ et $\mathbb{N}$

Nous avons vu dans la section précédente que le 10ème problème de Hilbert dans $\mathbb{N}$ n'avait pas de solutions. Mais comment transporter ce résultat dans $\mathbb{Z}$? En effet, a priori, dire qu'il n'existe pas d'algorithme déterminant l'existence de solutions entières positives d'un polynôme à coefficients entiers positifs n'implique pas qu'on connaisse un algorithme déterminant si il existe ou non des solutions entières à un polynôme à coefficients entiers. En effet, les racines de ce dernier polynôme pourrait être dans $\mathbb{Z}\backslash\mathbb{N}$.
Afin de pallier à ce problème, le théorème B.19 permet de définir de manière diophantienne $\mathbb{N}$ dans $\mathbb{Z}$, grâce au polynôme $\mathcal{Q}(U, X, Y, Z, T) = U - (X^2 + Y^2 + Z^2 + T^2)$. On obtient le théorème suivant :

Théorème 15. Le dixième problème de Hilbert n'a pas de solutions.

dem Supposons qu'il existe un algorithme permettant de décider si oui ou non il existe une racine entière à un polynôme de $\mathbb{Z}[X]$.
Alors, à tout polynôme $P(X_1, ..., X_N)$ de $\mathbb{N}[X_1, ..., X_N]$, on associe

$$P^*(X_1, ..., X_N, Y_{1,1}, ..., Y_{1,4}, ..., Y_{N,1}, ..., Y_{N,4}) = P(X_1, ..., X_N)^2 + \sum_{i=1}^{N} \mathcal{Q}(X_i, Y_{i,1}, Y_{i,2}, Y_{i,3}, Y_{i,4})^2.$$

On se rend compte qu'alors :

$$\exists (x_1, ..., x_N, y_{1,1}, ..., y_{N,4}) \in \mathbb{Z}^{5N}, P^*(x_1, ..., x_N, y_{1,1}, ..., y_{1,4}, ..., y_{N,1}, ..., y_{N,4}) = 0$$

équivaut à

$$\exists (x_1, ..., x_N, y_{1,1}, ..., y_{N,4}) \in \mathbb{Z}^{5N}, \begin{cases} P(x_1, ..., x_N) & = & 0 \\ \mathcal{Q}(x_1, y_{1,1}, y_{1,2}, y_{1,3}, y_{1,4}) & = & 0 \\ \vdots & & \\ \mathcal{Q}(x_1, y_{N,1}, y_{N,2}, y_{N,3}, y_{N,4}) & = & 0 \end{cases},$$

ce qui équivaut à :

$$\exists (x_1, ..., x_N) \in \mathbb{Z}^N, P(x_1, ..., x_N) = 0 \wedge x_1 \in \mathbb{N} \wedge ... \wedge x_N \in \mathbb{N}.$$

Donc, si on sait résoudre le problème de Hilbert sur $\mathbb{Z}$, on sait le résoudre sur $\mathbb{N}$. Or, on a montré que c'était impossible. Donc, le dixième problème de Hilbert n'admet pas de solutions dans $\mathbb{Z}$.

•

Remarque. Nous avons montré que dans $\mathbb{Z}$, muni de ses lois additive et multiplicative, le 10ème problème de Hilbert n'a pas de solutions. Donc, dans tout anneau isomorphe à $\mathbb{Z}$, le 10ème problème n'a encore pas de solutions.

5.2 Cas général

Cette partie n'est pas nécessaire pour les démonstrations des parties qui la suivront. Néanmoins, elle est utile à la compréhension de la méthode générale que nous allons suivre.

5.2.1 Définition diophantienne

– Pour un sous-ensemble :
Définition. Soit $(\mathcal{A}, +, \times)$ un anneau, et $\mathcal{B} \subset \mathcal{A}$. On dit que $\mathcal{B}$ est défini diophantiennement dans A si il existe un polynôme $P \in \mathcal{A}[X_0, X_1, ..., X_m]$ tel que :

$$b \in \mathcal{B} \Leftrightarrow \exists (x_1, ..., x_m) \in \mathcal{A}^m, P(b, x_1, ..., x_m) = 0_{\mathcal{A}}.$$

– Pour une simili-structure :
Définition. Soit $(\mathcal{A}, +_{\mathcal{A}}, \times_{\mathcal{A}})$ et $(\mathcal{B}, +_{\mathcal{B}}, \times_{\mathcal{B}})$ deux anneaux, tels que $B \subset A$. (a priori, les lois de $\mathcal{B}$ ne sont pas les restrictions des lois de $\mathcal{A}$). On dit alors que l'anneau $\mathcal{B}$ est défini diophantiennement dans l'anneau A si il existe trois entiers $n_{\mathcal{B}}, n_+, n_\times$, et trois polynômes $P_{\mathcal{B}} \in A[X_0, Y_1, ..., Y_{n_{\mathcal{B}}}]$, $P_+ \in A[X_0, X_1, X_2, Y_1, ..., Y_{n_+}]$, et $P_\times \in A[X_0, X_1, X_2, Y_1, ..., Y_{n_\times}]$ tel que :
- Pour tout $b \in \mathcal{A}$:
$$b \in \mathcal{B} \Leftrightarrow \exists (y_1, ..., y_{n_{\mathcal{B}}}) \in \mathcal{A}^{n_{\mathcal{B}}}, P_{\mathcal{B}}(b, y_1, ..., y_{n_{\mathcal{B}}}) = 0_{\mathcal{A}}.$$
- Pour tout $(b_1, b_2, b_3) \in \mathcal{B}^3$
$$b_1 = b_2 +_{\mathcal{B}} b_3 \Leftrightarrow \exists (y_1, ..., y_{n_+}) \in \mathcal{A}^{n_+}, P_+(b_1, b_2, b_3, y_1, ..., y_{n_+}) = 0_{\mathcal{A}}.$$
- Pour tout $(b_1, b_2, b_3) \in \mathcal{B}^3$
$$b_1 = b_2 \times_{\mathcal{B}} b_3 \Leftrightarrow \exists (y_1, ..., y_{n_\times}) \in \mathcal{A}^{n_\times}, P_\times(b_1, b_2, b_3, y_1, ..., y_{n_\times}) = 0_{\mathcal{A}}.$$

– Pour une relation :
Définition. Soit $(\mathcal{A}, +, \times)$ et B un sous-anneau de A. On dit qu'une relation est diophantienne sur $\mathcal{A}$ à coefficients dans B ssi la relation est définie sur A et si il existe un polynôme à coefficients dans B définissant la relation.

Remarque. L'intérêt de ces définitions est de pouvoir démontrer la généralisation du 10ème problème de Hilbert dans une « grosse »structure (dans la définition, $\mathcal{A}$), dès qu'on sait que le 10ème problème de Hilbert ne fonctionne pas dans la « petite »structure (dans la définition, $\mathcal{B}$).

5.2.2 Méthode générale

Théorème 16. Soit $(\mathcal{A}, +_{\mathcal{A}}, \times_{\mathcal{A}})$ et $(\mathcal{B}, +_{\mathcal{B}}, \times_{\mathcal{B}})$ deux anneaux, tels que $\mathcal{B}$ est défini diophantiennement dans $\mathcal{A}$. On suppose de plus que pour tout $P \in \mathcal{A}[X_1, ..., X_m]$, $Q \in \mathcal{A}[Y_1, ..., Y_n]$, il existe $R \in \mathcal{A}[X_1, ..., X_m, Y_1, ..., Y_n, W_1, ..., W_p]$ tel que :

$$\exists (x_1, ..., x_m, y_1, ..., y_m) \in \mathcal{A}^{n+m}, (P(x_1, ..., x_n) = 0 \wedge Q(y_1, ..., y_m) = 0)$$

$$\Leftrightarrow$$

$$\exists (x_1, ..., x_m, y_1, ..., y_n, w_1, ...w_p) \in \mathcal{A}^{p+m+n}, R(x_1, ..., x_m, y_1, ..., y_n, w_1, ...w_p) = 0$$

Alors : si le 10ème problème de Hilbert n'admet pas de solutions dans $\mathcal{B}$, alors il n'en admet pas dans $\mathcal{A}$.

dem On procède de la même façon que pour $\mathbb{N}$ et $\mathbb{Z}$. Supposons par l'absurde qu'il existe un algorithme permettant de dire, pour chaque polynôme $P \in \mathcal{A}[Z_1, ..., Z_k]$à coefficients dans $\mathcal{A}$, si il existe des k-uplets l'annulant ou pas.
Soit un polynôme $P \in \mathcal{B}[X_1, ..., X_n]$, qu'on note

$$P(X_1, ..., X_n) = \sum_{(i_1, ..., i_n) \in \mathbb{N}^n} a_{i_1, ..., i_n} X_1^{i_1} ... X_n^{i_n},$$

où toutes les opérations sont à prendre au sens de $\mathcal{B}$. On définit un polynôme $P^* \in \mathcal{A}[X_1, ..., X_n, Y_1, ..., Y_m]$ tel que, pour tout $(x_1, ..., x_n) \in \mathcal{A}^n$

$$\exists (y_1, ..., y_m) \in \mathcal{A}^m, P^*(x_1, ..., x_n, y_1, ..., y_m) = 0 \Leftrightarrow ((x_1, ..., x_n) \in \mathcal{B}^n \wedge P(x_1, ..., x_n) = 0)\,.$$

Donc on a résolu le 10ème problème de Hilbert dans $\mathcal{B}$, ce qui est absurde.

•

Remarque. On va utiliser la méthode précédente pour généraliser le 10ème problème de Hilbert. Dans les structures que l'on rencontrera, on va essayer de définir diophantiennement un avatar de $\mathbb{Z}$. Une fois cela fait, on aura montré que le 10ème problème de Hilbert n'admet pas de solutions dans la structure étudiée.

6 Cas des anneaux intègres de caractéristique nulle

On fixe R un anneau intègre de caractéristique nulle. On va chercher à montrer dans cette partie le théorème suivant :

Théorème 17. Il n'existe pas d'algorithme qui détermine si un polynôme P à coefficients dans $\mathbb{Z}[T]$ admet une « racine » $Q \in R[T]$ (i.e. $P(Q)(T) = 0$).

Lemme 6.1. Comme dans $\mathbb{Z}$, étant donné P et Q deux polynômes à coefficients $\mathbb{Z}[T]$, il existe deux polynômes G et H tels que : G s'annule équivaut à P s'annule et Q s'annule, et H s'annule équivaut à P ou Q s'annule.

dem On pose $H = PQ$ car R est intègre.
On pose $G = P^2 + TQ^2$. En effet, si G s'annule en un point noté $\overline{X}(T) \in R[T]$ (la barre signifie que ça peut être un n-uplet, avec n le nombre de variables de P et de Q). Alors : $P^2\left(\overline{X}(T)\right) = -TQ^2\left(\overline{X}(T)\right)$, et ceci est une égalité entre polynômes ! Donc, en regardant la valuation de T dans chacun de ces deux polynômes, on obtient qu'un pair est un impair (ce qui est absurde), sauf si $P^2\left(\overline{X}(T)\right) = Q^2\left(\overline{X}(T)\right) = 0$, et on conclut par intégrité de R.

•

Dans $R[T]$, on définit l'équation de Pell : (E) $X^2 - (T^2 - 1)Y^2 = 1$ (où X et Y sont des inconnues).

Remarque. Comme R est de caractéristique nulle, on peut injecter $\mathbb{Z}$ dans R. Mais cette injection n'est pas diophantienne. C'est pourquoi nous allons étudier l'équation de Pell, car dans $R[T]$ elle possède des solutions semblables à $\mathbb{Z}$, et elle va donc nous permettre de définir $\mathbb{Z}$ de manière diophantienne dans $R[T]$.

Notation. Pour faire cette étude, nous avons besoin d'un élément U (pris dans la clôture algébrique de $R(T)$) tel que $U^2 = T^2 - 1$. (De la même manière, nous utilisions $\sqrt{d}$ pour l'étude dans $\mathbb{Z}$).

Notation. On définit, pour tout $n \in \mathbb{N}$, X_n et Y_n les uniques éléments de $\mathbb{Z}[T]$, tels que $X_n + UY_n = (T + U)^n$.

Lemme 6.2. Les seules solutions de (E) dans $R[T]$ sont les $X = \pm X_n$ et $Y = \pm Y_n$, pour $n \in \mathbb{N}$.

dem On remarque que :

$$(E) \Leftrightarrow (X - UY)(X + UY) = 1.$$

– Or, comme on a :

$$X_n - UY_n = (T - U)^n = (T + U)^{-n},$$

les X_n et Y_n sont bien solutions de E dans $R[T]$.
– Réciproquement, montrons que ce sont les seules. Soit (X, Y) une solution de E dans $R[T]$, on pose $t = \dfrac{U}{T - 1}$, de manière à avoir la paramétrisation suivante :

$$T = \frac{t^2 + 1}{t^2 - 1}, \qquad U = \frac{2t}{t^2 - 1}.$$

Premièrement, on remarque que les seuls pôles possibles de $X+UY$ et $X-UY$, vues comme des fonctions de t, sont $+1$ et -1, car ce sont des polynômes en T et U, donc les pôles ne peuvent provenir que de la paramétrisation.
Deuxièmement, la remarque préliminaire nous dit que les zéros de $X-UY$ sont les pôles de $X+UY$ et réciproquement. Autrement dit, les seuls zéros possibles de $X-UY$ et $X+UY$, encore une fois vues comme des fonctions de t, sont -1 et 1. Donc, il existe $(n,k)\in\mathbb{Z}^2$ et un $c\in R^*$ tel que :

$$X+UY=c(t+1)^n(t-1)^k, \qquad X-UY=c^{-1}(t+1)^{-n}(t-1)^{-k}.$$

Troisièmement, on remarque que l'application $\begin{array}{cccc}\varphi & : & R(t) & \to & R(t)\\ & & P(t) & \mapsto & P(-t)\end{array}$ laisse T inchangé et envoie U sur $-U$. Donc, $\varphi\left(X+UY\right)=X-UY=c(-t+1)^n(-t-1)^k$.
Donc, $X-UY=c(-1)^{n+k}(t-1)^n(t+1)^k$. Par identification, $n=-k$, et $c^{-1}=c$ (donc $(c-1)(c+1)=0$), donc $c=\pm1$.
Finalement :

$$X+UY=\pm\left(\frac{t+1}{t-1}\right)^n=\pm(T+U)^n.$$

CQFD

•

Définition. On définit la relation d'équivalence $\sim$ sur $R[T]$ par :

$$\forall(P,Q)\in R[T]^2, P\sim Q\Leftrightarrow P(1)=Q(1).$$

Lemme 6.3. Pour tout $n\in\mathbb{N}$, $Y_n\sim n$.

dem Soit $n\in\mathbb{N}$. Puisque $(T+U)^n=X_n+UY_n$, on a :

$$Y_n=\sum_{\substack{i=1\\ i\text{ impair}}}^{n}\binom{i}{n}(T^2-1)^{(i-1)/2}T^n-i.$$

Ce qui donne le résultat.

•

Définition. On définit la relation unaire Imt par :

$$\mathrm{Imt}(Y)\Leftrightarrow Y\in R[T]\wedge\exists X\in R[T], X^2-(T^2-1)Y^2=1.$$

Lemme 6.4.
1. La condition $Z\sim 0$ est diophantienne sur $R[T]$ à coefficients dans $\mathbb{Z}[T]$.
2. Imt est diophantienne sur $R[T]$ à coefficients dans $\mathbb{Z}[T]$.
3. Si Y satisfait $\mathrm{Imt}(Y)$, alors il existe un entier $m\in\mathbb{N}$ tel que $Y\sim m$.
4. Pour tout $m\in\mathbb{N}$, il existe un polynôme $Y\in R[T]$ tel que $\mathrm{Imt}(Y)$ et $Y\sim m$.

dem
1. On définit $P(H,G)=G-(T-1)H$. Alors :
$$\forall Z\in R[T], Z\sim 0\Leftrightarrow\exists X\in R[T], P(Z,X)=0.$$
2. Evident, par définition de la relation.
3. Provient directement des lemmes précédents.
4. De même.

•

Nous sommes maintenant en mesure de démontrer le théorème 17, dont nous rappelons l'énoncé :

Théorème. Il n'existe pas d'algorithme qui détermine si un polynôme P à coefficients dans $\mathbb{Z}[T]$ admet une « racine » $Q \in R[T]$ (i.e. $P(Q)(T) = 0$).

dem du théorème 17.
Supposons qu'il existe un algorithme résolvant le 10ème problème de Hilbert dans $R[T]$ à coefficients dans $\mathbb{Z}[T]$. Or, avec ce que nous avons vu précédemment, nous pouvons, à partir d'un polynôme à coefficients entiers, noté $P(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$, construire un polynôme $P^*(Q_1, ..., Q_m) \in \mathbb{Z}[T][X_1, ..., X_m]$, à coefficients dans $\mathbb{Z}[T]$ tel que :

$$\exists (z_1, ..., z_n) \in \mathbb{Z}^n, P(z_1, ..., z_n) = 0 \Leftrightarrow \exists (Z_1, ..., Z_m) \in R[T]^m, P^*(Z_1, ..., Z_m) = 0.$$

En effet, on a :

$$\exists (z_1, ..., z_n) \in \mathbb{Z}^n, P(z_1, ..., z_n) = 0 \Leftrightarrow (\exists (Z_1, ..., Z_n) \in R[T]^n, \mathrm{Imt}(Z_1) \wedge \mathrm{Imt}(Z_2) \wedge ... \wedge \mathrm{Imt}(Z_n) \wedge P(Z_1, ..., Z_n) \sim 0),$$

ce qui est prouvé en prenant Z_1, ..., Z_n des polynômes tels que $Z_i \sim z_i$, ce qu'on peut faire d'après le lemme précédent. Et comme Imt et $\sim$ sont des relations diophantiennes sur $R[T]$ à coefficients dans $\mathbb{Z}[T]$, on peut en déduire un polynôme P^* vérifiant ce qu'on veut.
Donc, à partir d'un algorithme pour $R[T]$ à coefficients dans $\mathbb{Z}[T]$, on en déduit un algorithme pour Z, ce qui n'est pas possible.

•

Remarque. La méthode utilisée précédemment correspond à la méthode générale présentée dans la partie précédente. Dans la preuve, on montre en effet que $\mathbb{Z}$ est définie diophantiennement dans $R[T]$:

$$\mathbb{Z} = \{P \in R[T] | \mathrm{Imt}(P)\} / \sim .$$

En prenant comme loi, les lois induites par le quotient. (A des fins de lisibilité, nous avons dans la preuve précédente explicité l'argument)

7 Cas de certains corps de fractions rationnelles

Dans cette section, on s'intéresse au problème diophantien de $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$, avec $\mathbb{K}$ un corps formellement réel, i.e., un corps tel que $-1_{\mathbb{K}}$ n'est pas une somme de carrés.
Afin d'étudier le problème diophantien sur $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$, nous allons passer par les courbes elliptiques et définir $\mathbb{Z}$ diophantiennement à partir de celles-ci. Pour cela, soit $E_0 : y^2 = x^3 + ax + b$ une courbe elliptique avec $(a, b) \in \mathbb{Q}^2$, tel que $j(a, b)$ non entier, alors $E_0(\mathbb{Q})$ est sans multiplication complexe, d'après le théorème C.21.
On définit $E : (T^3 + aT + b)Y^2 = X^3 + aX + b$.

Lemme 7.1. Soit $\mathbb{L}$ un corps de caractérisque 0. Soit $P_1 = (T, 1)$ (point de la courbe $E(\mathbb{L}(T))$). Alors P_1 est d'ordre infini et génère le groupe $E(K(T))$ modulo les éléments d'ordre 2, i.e., pour tout $P \in E(\mathbb{K}(T))$, il existe $n \in \mathbb{Z}$ et $R \in E(K(T))$ tel que $2R = 0$, tel que $Q - n \cdot P_1 = R$.

dem Pour faire la preuve, nous allons avoir besoin de naviguer entre les fractions rationnelles (formelles) et les fonctions rationnelles. Puisque $\mathbb{K}$ est de caractéristique nulle, la correspondance est valide.
On identifie la fonction rationnelle $\begin{array}{ccc} E_0(\mathbb{K}) & \to & \mathbb{K} \\ (x, y) & \mapsto & x \end{array}$ à l'indéterminée T, et on appelle U l'indéterminée qui permet de faire l'identification avec $\begin{array}{ccc} E_0(\mathbb{K}) & \to & \mathbb{K} \\ (x, y) & \mapsto & y \end{array}$. On a alors $U^2 = T^3 + aT + b$. En effet :

$$\forall (x, y) \in E_0(\mathbb{K}), (U^2 - T^3 - aT - b)(x, y) = y^2 - x^3 - ax - b = 0.$$

On pose $F = \mathbb{K}(T, U)$. Grâce à la correspondance, F correspond à

$$\{f : E_0(\mathbb{K}) \to \mathbb{K} \,|\, \exists P \in \mathbb{K}(T, U), \forall (x, y) \in E_0(\mathbb{K}), f(x, y) = P(x, y)\}.$$

On définit

$$\begin{array}{rccc} \psi_1 & : & E(F) & \to & E_0(F) \\ & & (X,Y) & \mapsto & (X,UY) \end{array}.$$

Autrement dit, pour tout $(x,y) \in \mathbb{K}^2$, pour tout $(X,Y) \in E(F)$,

$$\psi_1(X,Y)(x,y) = (X(x,y), U(x,y)Y(x,y)) = (X(x,y), yY(x,y)).$$

Puisque ψ_1 est à coordonnées rationnelles et que $\psi_1(0_{\mathbb{K}(F)}) = 0_{\mathbb{K}(F)}$, ψ_1 est un homomorphisme de groupes, d'après le théorème C.22.
Désormais, on note $\mathrm{Rat}_{\mathbb{K}}(E_0, E_0)$ l'ensemble des fonctions $E_0(\mathbb{K}) \to E_0(\mathbb{K})$ telles que les coordonnées soient des fractions rationnelles de F. On définit, la fonction ψ_2 comme étant la fonction qui permet de faire explicitement la correspondance entre les fractions de F et les fonctions rationnelles associées, autrement dit :

$$\begin{array}{rccc} \psi_2 & : & E_0(F) & \to & \mathrm{Rat}_{\mathbb{K}}(E_0,E_0) \\ & & (V,W) & \mapsto & ((x,y) \mapsto (V(x,y), W(x,y))) \end{array}.$$

C'est clairement un morphisme. Donc, $\varphi = \psi_2 \circ \psi_1$ est un morphisme également, et il vaut :

$$\begin{array}{rccc} \varphi & : & E(F) & \to & \mathrm{Rat}_{\mathbb{K}}(E_0,E_0) \\ & & (V,W) & \mapsto & ((x,y) \mapsto (V(x,y), yW(x,y))) \end{array}.$$

On note ψ la restriction de φ à $E(\mathbb{K}(T))$ (vu comme un sous-ensemble de $E(F)$). On remarque qu'on a alors, pour tout $(X,Y) \in E(\mathbb{K}(T))$:

$$T \circ \psi(X,Y) = X, \tag{13}$$
$$U \circ \psi(X,Y) = U \cdot Y. \tag{14}$$

Donc, ψ est injective (et est encore un morphisme).
D'après le théorème C.22, on a :

$$\mathrm{Rat}_{\mathbb{K}}(E_0,E_0) = \mathrm{End}_{\mathbb{K}}(E_0) \oplus E_0(\mathbb{K}).$$

Et ce, en identifiant $E_0(\mathbb{K})$ aux fonctions constantes égales à un élément de $E_0(\mathbb{K})$. Or, E_0 est sans multiplication complexe, d'où, en notant, pour tout $m \in \mathbb{Z}$, $\begin{array}{rccc} \alpha_m & : & E_0(\mathbb{K}) & \to & E_0(\mathbb{K}) \\ & & P & \mapsto & m \cdot P \end{array}$, on a :

$$\mathrm{Rat}_{\mathbb{K}}(E_0,E_0) = \{\alpha_m | m \in \mathbb{Z}\} \oplus E_0(\mathbb{K}).$$

Nous allons nous intéresser successivement à $\psi^{-1}[\{\alpha_m | m \in \mathbb{Z}\}]$ et $\psi^{-1}[E_0(\mathbb{K})]$

- Pour le premier, on remarque que :

  $$\forall (x,y) \in E_0(\mathbb{K}), \psi(P_1)(x,y) = (T(x,y), y) = (x,y) = \alpha_1(x,y).$$

  Et comme ψ est un morphisme, on a que pour tout $m \in \mathbb{Z}$, $\psi(m \cdot P_1) = m \cdot \alpha_1 = \alpha_m$. En particulier, P_1 est d'ordre infini.

- Pour le second, considérons $(X,Y) \in \psi^{-1}[E_0(\mathbb{K})]$. En remplaçant ψ par son expression, on obtient que $\psi(X,Y) = [(x,y) \mapsto (X(x,y), yY(x,y))]$ est une fonction constante, donc :
  - X est une fonction constante, et donc, il existe $c \in \mathbb{K}$ tel que $X^3 + aX + b = c$.
  - (X,Y) étant un point de la courbe elliptique $E(\mathbb{K}(T))$, on a $(T^3 + aT + b)Y^2 = X^3 + aX + b = c$, donc $Y = 0$, car sinon, on obtient deux fractions en T de degrés de parité différente qui sont égales.

  Et comme $Y = 0$, (X,Y) est un point d'ordre 2 sur la courbe $E(\mathbb{K}(T))$.
- Concluons. Soit $Q \in E(\mathbb{K}(T))$ quelconque. Alors, il existe $n \in \mathbb{Z}$, et $r \in E_0(\mathbb{K})$ tel que $\psi(Q) = \alpha_n + r$. Alors, comme $\alpha_n = \psi(n \cdot P_1)$, et ψ est un morphisme, $\psi(Q - n \cdot P_1) = r$. Donc $Q - n \cdot P_1$ est un élément d'ordre 2.

•

Notation. On note, pour tout $n \in \mathbb{N}$, $(X_n, Y_n) = n \cdot P_1$. On remarque que $(X_n, Y_n) \in \mathbb{Q}(T)^2$.

Définition. On définit la relation d'équivalence $\sim$ par, pour tout $(V, W) \in \mathbb{K}(T)^2$, $V \sim W$ si et seulement si $V - W$ prend la valeur 0 en l'infini. (En considérant V et W comme des fonctions rationnelles sur la droite projective)

Lemme 7.2. Avec toutes les notations précédentes :

$$\forall m \in \mathbb{Z}\backslash\{0\}, \frac{X_m}{TY_m} \sim m.$$

dem D'après le théorème C.23, on a directement :

$$\left(\frac{(T/U) \circ \alpha_m}{T/U}\right)(0) = m \cdot 1_{\mathbb{K}}.$$

En définissant ψ les mêmes notations que dans la démonstration précédente, d'après l'équation 13, on a : $X_m = T \circ \psi(X_m, Y_m) = T \circ \alpha_m$, et d'après l'équation 14, on a :

$$Y_m = \frac{U \circ \psi(X_m, Y_m)}{U} = \frac{U \circ \alpha_m}{U},$$

donc,

$$\frac{X_m}{TY_m} = \frac{T \circ \alpha_m}{T \cdot (U \circ \alpha_m)/U} = \frac{(T/U) \circ \alpha_m}{T/U}.$$

Et le résultat s'ensuit.

•

Définition. On définit la relation unaire Imt par :

$$\forall Z \in \mathbb{K}(T), \mathrm{Imt}(Z) \Leftrightarrow \left(Z = 0 \vee \exists (X, Y) \in \mathbb{K}(T)^2, ((X, Y) \in 2E(\mathbb{K}(T)) \wedge 2TYZ = X)\right).$$

Lemme 7.3.
1. La relation Imt est diophantienne dans $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$.
2. Si Z vérifie $\mathrm{Imt}(Z)$, alors il existe $m \in \mathbb{Z}$, tel que $Z \sim m$.
3. Pour tout entier m, il existe $Z \in \mathbb{Q}(T)$ qui vérifie $\mathrm{Imt}(Z)$ et $Z \sim m$.

dem

1. Voir l'expression de α_2 en termes de fractions rationnelles (théorème C.24), ce qui permet de définir diophantiennement notre relation.
2. Soit $Z \in \mathbb{K}(T)$, tel que $\mathrm{Imt}(Z)$. Alors, ou bien $Z = 0$, et alors le résultat est prouvé, ou bien il existe $(X, Y) \in \mathbb{K}(T)$, et $(X', Y') \in E(\mathbb{K}(T))$, tel que $(X, Y) = 2 \cdot (X', Y')$ (où $\cdot$ est la loi de groupe de la courbe elliptique), et $Z = \dfrac{X}{2TY}$.
   D'après le lemme 7.1, il existe $n \in \mathbb{Z}$ et $R \in E(\mathbb{K}(T))$ un point d'ordre 2 tel que : $(X', Y') = n \cdot P_1 + R = (X_n, Y_n) + R$ dans $E(\mathbb{K}(T))$. Donc $(X, Y) = (2n) \cdot P_1 + 0 = (X_{2n}, Y_{2n})$. D'où :
   $$Z = \frac{X_{2n}}{2TY_{2n}} \sim n$$
   (le calcul étant fait dans $\mathbb{K}(T)$)
3. Si $m = 0$, on prend $Z = 0$. Sinon, on prend
   $$Z = \frac{X_{2m}}{2TY_{2m}}$$

•

Remarque. Cette dernière relation permet de coder les entiers, puisqu'il suffit d'évaluer en ∞ les fractions de $\mathbb{K}(T)$ qui vérifient la relation Imt. (en les assimilant à des fonctions de la droite projective)
Néanmoins, nous ne savons pas encore coder l'évaluation en l'infini de manière diophantienne, ce à quoi nous allons désormais nous atteler.

Définition. On définit la relation unaire Com par :

$$\forall y \in \mathbb{K}(T), \mathrm{Com}(y) \Leftrightarrow \exists x \in \mathbb{K}(T), y^2 = x^3 - 4.$$

On admet le lemme suivant :

Lemme 7.4.
1. La relation Com est diophantienne sur $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}$.
2. Soit $y \in \mathbb{K}(T)$ tel que $\mathrm{Com}(y)$, alors $y \in \mathbb{K}$.
3. Pour tout $z \in \mathbb{Q}$, il existe $y \in \mathbb{Q}$ tel que $\mathrm{Com}(y)$ et $y > z$.

Remarque. Le choix de la courbe elliptique $y^2 = x^3 - 4$ pour la définition de Com s'explique par le fait que $y^2 = x^3 - 4$ vérifie les deux points suivants, prouvés dans [5] :
- Elle n'admet pas de paramétrisation rationnelle.
- Le groupe de ses points rationnels est infini.

Toute autre courbe elliptique vérifiant ces deux propriétés aurait convenu.

Définition. On définit la relation unaire $\dot{\sim} 0$ par :

$$\forall Z \in \mathbb{K}(T), Z \dot{\sim} 0 \Leftrightarrow \exists (X_1, X_2, X_3, X_4, X_5, y) \in \mathbb{K}(T)^6, \left(\mathrm{Com}(y) \wedge (y - T)Z^2 + 1 = X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2\right).$$

Remarque. Le choix de la notation pour cette relation unaire provient du fait qu'elle va avoir de forts liens avec ~ 0. Mais on pourrait de plus en déduire une relation binaire comparable à $\sim$.

Lemme 7.5.
1. La relation $\dot{\sim} 0$ est diophantienne sur $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$.
2. Si $\mathbb{K}$ est formellement réel, et si $Z \dot{\sim} 0$, alors $Z \sim 0$.
3. Si $Z \in \mathbb{Q}(T)$ et $Z \sim 0$, alors $Z \dot{\sim} 0$.

dem

1. est évident.
2. Soit $Z \in \mathbb{K}(T)$ tel que $Z \dot{\sim} 0$, et $\mathbb{K}$ formellement réel. Il existe $(X_1, X_2, X_3, X_4, X_5, y) \in \mathbb{K}(T)^6$ tel que $\mathrm{Com}(y)$ et $(y - T)Z^2 + 1 = X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2$.
   Supposons par l'absurde que $Z \not\sim 0$, alors $\deg Z \geq 0$ ($\deg$ étant le degré d'une fonction rationnelle), car $\sim$ représente la limite en l'infini, et pour que cette limite soit 0, il faut que le degré soit négatif. D'après le lemme précédent, $y \in \mathbb{K}$ car y vérifie $\mathrm{Com}(y)$, donc $(y - T)Z^2 + 1$ est de degré positif et impair, mais le degré de $X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2$ est pair car le corps est formellement réel, ce qui conduit à une contradiction.
3. Soit $Z \in \mathbb{Q}(T)$ tel que $Z \sim 0$. Alors $TZ^2 \sim 0$ (il suffit de considérer le degré de TZ^2). Par définition en l'infini, il existe M rationnel positif tel que :

   $$\forall x \in \mathbb{R}, |x| \geq M \Rightarrow \left|(TZ^2)(x)\right| \leq \frac{1}{2}.$$

   Par le lemme précédent, il existe $y \in \mathbb{Q}$ qui vérifie $\mathrm{Com}(y)$ et $y > M \geq 0$. Alors, on a :

   $$\forall x \in \mathbb{R}, ((y - T)Z^2 + 1)(x) \geq 0.$$

   En effet, si $|x| \geq y$, alors $(-TZ^2 + 1) \geq 0$ et yZ^2 est positif, et sinon, $(y - T)(x) \geq 0$.
   On écrit $Z = \frac{A}{B}$, avec $(A, B) \in \mathbb{Q}[T]^2$. Alors, pour tout $x \in \mathbb{Q}$, $((y-T)A^2+B^2)(x) \geq 0$. Donc, d'après le théorème B.20, il existe $(P_1, P_2, P_3, P_4, P_5) \in \mathbb{Q}[T]^5$ tel que $(y-T)A^2+B^2 = P_1^2+P_2^2+P_3^2+P_4^2+P_5^2$. Donc, $(y - T)Z^2 + 1$ est somme de cinq carrés dans $Q(T)$ (en redivisant par B^2). Donc $Z \dot{\sim} 0$.

•

Théorème 18. Le problème diophantien dans $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$ n'admet pas de solutions.

dem On a montré que $\mathbb{Z}$ est défini diophantiennement dans $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$. A partir d'un polynôme P à coefficients dans $\mathbb{Z}$, on peut former un polynôme P^* à coefficients dans $\mathbb{Z}[T]$ tel que :

$$\exists(z_1, ..., z_n) \in \mathbb{Z}^n, P(z_1, ..., z_n) = 0 \Leftrightarrow \exists(Z_1, ..., Z_m) \in \mathbb{K}(T)^m, P^*(Z_1, ..., Z_m) = 0.$$

Pour prouver cela, on remarque que :

$$\exists(z_1, ..., z_n) \in \mathbb{Z}^n, P(z_1, ..., z_n) = 0 \Leftrightarrow \exists(Z_1, ..., Z_n) \in \mathbb{K}(T)^n, (\mathrm{Imt}(Z_1) \wedge ... \wedge \mathrm{Imt}(Z_n) \wedge P(Z_1, ..., Z_n) \dot{\sim} 0).$$

Et puisque toutes les relations sont diophantiennes dans $\mathbb{K}(T)$ à coefficients dans $\mathbb{Z}[T]$, et que $\wedge$ se comporte correctement avec le caractère diophantien des relations (car $\mathbb{K}(T)$ est un anneau intègre), le théorème est démontré.

•

Conclusion

Dans la première partie du mémoire, nous avons traité le cas de $\mathbb{Z}$ et de $\mathbb{N}$ du 10ème problème de Hilbert. À cette fin, nous avons étudié les équations de Pell, qui nous ont permis de démontrer le point clé, qui est que le graphe de l'exponentielle est diophantien. Nous avons également pu coder les suites finies de manière diophantienne, et donc, à partir de là, démontrer l'équivalence entre fonctions récursives totales et fonctions diophantiennes, nous permettant de conclure avec des résultats de logique.
Puis, dans une seconde partie, nous avons généralisé le résultat à d'autres structures, à l'intérieur desquelles nous avons cherché à définir $\mathbb{Z}$ de telle manière à ce que le résultat sur ces structures découle du résultat de la première partie. Pour ce faire, nous avons utilisé une équation de Pell et des courbes elliptiques (méthode qui est souvent utilisée dans le cadre de l'étude du 10ème problème de Hilbert).

A Les 24 lemmes

Soit $a \in \mathbb{N}^*$, soit $d = a^2 - 1$, tel que $\sqrt{d}$ ne soit pas entier. On note $E_a = \{(x, y) \in \mathbb{N}^2 \,|x^2 - dy^2 = 1\}$, et $F_a = \{(x, y) \in \mathbb{Z}^2 \,|x^2 - dy^2 = 1\}$.

1. Pour tout $(x, y) \in F_a$, on ne peut pas avoir $1 < x + y\sqrt{d} < a + \sqrt{d}$.
2. Pour tous $(x, y) \in F_a$ et $(x', y') \in F_a$, on définit $(x'', y'') \in \mathbb{Z}^2$ les uniques entiers tels que $x'' + y''\sqrt{d} = (x + y\sqrt{d})(x' + y'\sqrt{d})$. Alors $(x'', y'') \in F_a$.
3. On définit, pour tout $n \in \mathbb{N}$, $x_n(a), y_n(a)$ (aussi notés x_n et y_n si il n'y a pas d'ambuiguïtés) les uniques entiers tels que $x_n(a) + y_n(a)\sqrt{d} = (a + \sqrt{d})^n$. Alors, pour tout $n \in \mathbb{N}$, $(x_n, y_n) \in E_a$.
4. $E_a = \{(x_n(a), y_n(a)) | n \in \mathbb{N}\}$.
5. Pour tout $(m, n) \in \mathbb{N}^2$, $x_{m\pm n} = x_m x_n \pm d y_n y_m$ et $y_{m\pm n} = x_n y_m \pm x_m y_n$.
6. Pour tout $m \in \mathbb{N}$, $x_{m\pm 1} = a x_m \pm d y_m$, et $y_{m\pm 1} = a y_m \pm x_m$.
7. Pour tout $n \in \mathbb{N}$, $\text{pgcd}(x_n, y_n) = 1$.
8. Pour tout $(n, k) \in \mathbb{N}^2$, $y_n | y_{nk}$.
9. Pour tout $(n, t) \in \mathbb{N}^2$, $y_n | y_t \Leftrightarrow n | t$.
10. Pour tout $(n, k) \in \mathbb{N}^2$, $y_{nk} \equiv k x_n^{k-1} y_n \ \left[\text{mod } (y_n)^3\right]$.
11. Pour tout $n \in \mathbb{N}$, $y_n^2 | y_{n y_n}$.
12. Pour tout $(n, t) \in \mathbb{N}^2$, si $y_n^2 | y_t$, alors $y_n | t$.
13. Pour tout $n \in \mathbb{N}$, $x_{n+1} a x_n - x_{n-1}$ et $y_{n+1} = a y_n - y_{n-1}$.
14. Pour tout $n \in \mathbb{N}$, $y_n \equiv n \ [\text{mod } a - 1]$.
15. Pour tout $(a, b, c) \in \mathbb{N}^3$, si $a \equiv b \ [\text{mod } c]$ alors pour tout $n \in \mathbb{N}$, $x_n(a) \equiv x_n(b) \ [\text{mod } c]$ et $y_n(a) \equiv y_n(b) \ [\text{mod } c]$.
16. Pour tout $n \in \mathbb{N}$, $2 | n \Leftrightarrow 2 | y_n$.
17. Pour tout $n \in \mathbb{N}$, $x_n(a) - y_n(a)(a - y) \equiv y^n \ \left[\text{mod } 2ay - y^2 - 1\right]$.
18. Pour tout $n \in \mathbb{N}$, $y_{n+1} > y_n \geq n$.
19. Pour tout $n \in \mathbb{N}$, $x_{n+1}(a) > x_n(a) \geq a^n$, et $x_n(a) \leq (2a)^n$.
20. Pour tout $(n, j) \in \mathbb{N}^2$, $x_{2n\pm j} \equiv -x_j \ [\text{mod } x_n]$.
21. Pour tout $(n, j) \in \mathbb{N}^2$, $x_{4n\pm j} \equiv x_j \ [\text{mod } x_n]$.
22. Soit $(i, j, n) \in \mathbb{N}^3$ tel que $x_i \equiv x_j \ [\text{mod } x_n]$ et $i \leq j \leq 2n$ et $n > 0$. Alors, $i = j$ ou ($a = 2$ et $n = 1$ et $i = 0$ et $j = 2$).
23. Soit $(i, j, n) \in \mathbb{N}^3$ tel que $x_i \equiv x_j \ [\text{mod } x_n]$ et $n > 0$ et $0 < i \leq n$ et $0 \leq j < 4n$. Alors $j \in \{i, 4n - i\}$.
24. Si $0 < i \leq n$ et $x_i \equiv x_j \ [\text{mod } x_n]$ alors $j \equiv \pm i \ [\text{mod } 4n]$.

B Les sommes de carrés

Nous allons ici démontrer le théorème de Lagrange, et mentionner un autre théorème important de décomposition en somme de carrés.

Théorème 19. Soit $n \in \mathbb{Z}$.

$$n \in \mathbb{N} \Leftrightarrow \exists (a,b,c,d) \in \mathbb{Z}^4, n = a^2+b^2+c^2+d^2.$$

Pour ce faire nous avons besoin de trois lemmes.

Lemme B.1. Pour tout $(x_1,x_2,y_1,y_2,z_1,z_2,t_1,t_2) \in \mathbb{N}^8$:

$$\begin{array}{rcl} (x_1^2+y_1^2+z_1^2+t_1^2)(x_2^2+y_2^2+z_2^2+t_2^2) & = & (x_1x_2+y_1y_2+z_1z_2+t_1t_2)^2 \quad + \quad (x_1y_2-y_1x_2+t_1z_2-z_1t_2)^2 \\ & + & (x_1z_2-z_1x_2+y_1t_2-t_1y_2)^2 \quad + \quad (x_1t_2-t_1x_2+z_1y_2-y_1z_2)^2. \end{array}$$

dem On développe tout.

•

Lemme B.2. Pour tout nombre premier p impair, il existe $(a,b) \in \mathbb{N}^2$ tel que $p|1+a^2+b^2$.

dem Tous les éléments de l'ensemble $\left\{ a^2 \middle| a \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right] \right\}$ sont incrongus deux à deux modulo p, et de même pour tous les éléments de l'ensemble $\left\{ -b^2-1 \middle| b \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right] \right\}$. Donc, par le principe des tiroirs, il existe $(a,b) \in \left[\!\left[0, \frac{p-1}{2} \right]\!\right]^2$ tel que $a^2 \equiv -b^2-1 \pmod{p}$. Donc, il existe $n \in \mathbb{N}$ tel que $a^2+b^2+1^2+0^2 = np$, et d'après l'encadrement sur a et b, on a que $0 < n < p$.

•

Lemme B.3. Tout nombre premier impair p est somme de quatre carrés.

dem Soit p un nombre premier impair. Soit m le plus petit entier positif tel que mp est une somme de carrés. (D'après la démonstration précédente, $m < p$) On note $mp = x_1^2+x_2^2+x_3^2+x_4^2$. Supposons par l'absurde que $m > 1$.
Pour tout $i \in [\![1,4]\!]$, il existe un unique $y_i \in \left[\!\left[\frac{-m+1}{2}, \frac{m}{2} \right]\!\right]$. On a alors qu'il existe $r \in [\![0,m]\!]$ tel que $y_1^2+y_2^2+y_3^2+y_4^2 = rm$. Montrons que $r < m$. Supposons par l'absurde que $r = m$, donc pour tout $i \in [\![1,4]\!]$, $y_i = \frac{m}{2}$. Alors, pour tout $i \in [\![1,4]\!]$, il existe $k_i \in \mathbb{Z}$ tel que $x_i = \frac{m}{2} + k_i m$, alors

$$x_i^2 = y_i^2 + 2 \times \frac{m}{2} k_i m + k_i^2 m^2$$

Donc, $mp = m^2 + (k_1+k_2+k_3+k_4)m^2 + (k_1^2+k_2^2+k_3^2+k_4^2)m^2$, d'où $m|p$ ce qui n'est pas possible car p premier et $p > m > 1$ par hypothèse.
Finalement, on obtient $mp \times mr = z_1^2+z_2^2+z_3^2+z_4^2$ en utilisant l'identité des quatre carrés, avec chaque z_i divisible par m d'après la formule, et on pose alors pour tout $i \in [\![1,4]\!]$, $w_i = \frac{z_i}{m}$, et on obtient $w_1^2+w_2^2+w_3^2+w_4^2 = rp$, avec $r < m$, ce qui est absurde par minimalité de m.
Donc, $m = 1$.

•

dem du théorème de Lagrange. Comme $2 = 1^2+1^2+0^2+0^2$, l'identité des quatre carrés nous permet de conclure car tout nombre premier impair est somme de quatre carrés.

•

Théorème 20. Tout polynôme à coefficients rationnels à une variable positif est somme de cinq carrés dans $\mathbb{Q}[T]$, voir [4].

C Les courbes elliptiques

Soit $\mathbb{K}$ un corps de caractéristique différente de 2 et 3.
Une courbe elliptique E est une courbe de la forme : $y^2 = x^3 + ax + b$, avec $(a, b) \in \mathbb{K}^2$.
Pour tout $\mathbb{L}$ surcorps de $\mathbb{K}$, on note $E(\mathbb{L}) = \left\{(x, y) \in \mathbb{L}^2 \,\middle|\, y^2 = x^3 + ax + b\right\} \cup \{\infty\}$. (On peut aussi la définir, directement dans le plan projectif : $E(\mathbb{L}) = \left\{[x, y, z] \in \mathbb{P}^2(\mathbb{L}) \,\middle|\, y^2 z = x^3 + axz^2 + bz^3\right\}$)
Si $4a^3 + 27b^2 \neq 0$, on peut définir une loi de groupe sur $E(\mathbb{L})$, dont ∞ (ou $[0, 1, 0]$) est le neutre tel que, si P, Q et R sont trois points alignés, alors $P + Q + R = 0$ (0 symbolisant le neutre du groupe, i.e. $0 = \infty = [0, 1, 0]$). Et, si $R = [x, y, z]$, alors $-R = [x, -y, z]$. On note $\mathrm{End}_{\mathbb{L}}(E)$ l'ensemble des endomorphismes de groupe de $E(\mathbb{L})$, tels que les fonctions coordonnés sont des fraction rationnels. En d'autres mots, c'est l'ensemble des $\alpha \in E(\mathbb{L})^{E(\mathbb{L})}$ tel que α est un endomorphisme de groupe de $E(\mathbb{L})$ et tel qu'il existe $(R_1, R_2) \in \overline{\mathbb{L}}(X, Y)^2$ (avec $\overline{\mathbb{L}}$ la clôture algébrique de $\mathbb{L}$), tel que

$$\forall (x, y) \in E(\mathbb{L}), \alpha((x, y)) = (R_1(x, y), R_2(x, y))$$

Si $\mathrm{End}_{\mathbb{L}}(E) = \{P \mapsto n \cdot P | n \in \mathbb{Z}\}$, on dit que $E(\mathbb{L})$ est sans multiplication complexe. (on précise que $n \cdot P = \underbrace{P + ... + P}_{\text{n fois}}$)
Pour tous les théorèmes qui suivent, voir [3] pour une démonstration.

Théorème 21. Soit $E : y^2 = x^3 + ax + b$, avec $(a, b) \in \mathbb{Q}^2$. On observe que si $j = \dfrac{2^8 3^3 a^3}{4a^3 + 27b^2}$ est non entier, alors $E(\mathbb{C})$ est sans multiplication complexe.

Théorème 22. Soit $\mathbb{K}$ un corps. Soit $E : y^2 = x^3 + ax + b$, avec $(a, b) \in \mathbb{K}^2$. Alors tout fonction $\psi : E(\mathbb{K}) \to E(\mathbb{K})$ ayant pour fonctions coordonnées des fractions rationnelles est la translatée d'un morphisme de groupes.

Théorème 23. Pour toute courbe elliptique E définie sur un corps $\mathbb{K}$, vue dans le plan projectif, en notant $\begin{array}{ccccc} f & : & E(\mathbb{K}) & \to & \mathbb{K} \\ & & [x, y, z] & \mapsto & x \end{array}$ et $\begin{array}{ccccc} g & : & E(\mathbb{K}) & \to & \mathbb{K} \\ & & [x, y, z] & \mapsto & y \end{array}$, et en notant, pour tout $n \in \mathbb{Z}$, $\begin{array}{ccccc} \alpha_n & : & E(\mathbb{K}) & \to & E(\mathbb{K}) \\ & & P & \mapsto & n \cdot P \end{array}$ on a :

$$\frac{(g/f) \circ \alpha_n}{g/f}([0, 1, 0]) = n \cdot 1_{\mathbb{K}}$$

Théorème 24. Avec les mêmes notations que précédemment, en notant $\alpha_2((X, Y)) = (R_1(X, Y), R_2(X, Y))$, on a :

$$R_1(X, Y) = \left(\frac{3X^2 + a}{2Y}\right)^2 - 2X$$

$$R_2(X, Y) = \left(\frac{3X^2 + a}{2Y}\right)\left(3X - \left(\frac{3X^2 + a}{2Y}\right)^2\right) - Y$$

Références

[1] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, vol 80, no. 3*, pages 233–269, March 1973.

[2] J. Denef. The diophantine problem for polynomial rings and fields of rational functions. *Transactions of the American Mathematical Society, vol 242*, pages 391–399, August 1978.

[3] Serge Lang. *Elliptic Functions*. Addison-Wesley, 1973.

[4] Yves Pourchet. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arithmetica, vol 19*, pages 89–104, 1971.

[5] R. M. Robinson. The undecidability of pure transcendental extensions of real fields. *Z. Math. Logik Grundlagen Math, vol 10*, pages 275–282, 1964.