Julia Robinson

Julia Robinson a été la première femme mathématicienne à être élue à l'Académie nationale des sciences et la première femme présidente de la American Mathematical Society. Elle a apporté des contributions à la théorie des jeux et aux problèmes de décision, mais elle est surtout renommée pour ses travaux fondamentaux sur le dixième problème de Hilbert. Le mathématicien influent David Hilbert a publié au début du vingtième siècle une liste de problèmes qu'il pensait devoir guider la recherche pour ce siècle. La plupart des problèmes sont désormais au moins partiellement résolus, bien qu'il en reste quelques-uns célèbres (le plus évident étant le huitième problème, connu sous le nom d'hypothèse de Riemann). Celle-ci énonce simplement que la partie réelle d'un zéro non trivial de la fonction zêta de Riemann est toujours 1/2. La fonction zêta de Riemann est une fonction d'une variable complexe $z = a + ib$ qui, dans le cas où $\mathrm{Re}(z) > 1$, peut s'écrire sous forme de série infinie convergente :

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}.$$

Techniquement parlant, ce qui précède est un cas très particulier de ce que l'on appelle une série de Dirichlet, et la fonction zêta de Riemann est le prolongement analytique de cette fonction à tout le plan complexe. Toute fonction arithmétique peut être associée à une série de Dirichlet infinie qui est la fonction génératrice de cette fonction :

$$D_f(z) = \sum_{n=1}^{\infty} \frac{f(n)}{n^z}.$$

Dans le cas où $\mathrm{Re}(z) > 1$, la fonction zêta de Riemann peut être représentée comme un produit d'Euler :

$$\zeta(z) = \prod_p \frac{1}{1 - \frac{1}{p^z}}.$$

C'est l'expression du fait que les entiers naturels peuvent être factorisés de manière unique en puissances de nombres premiers.

Une fonction arithmétique est une fonction définie uniquement sur les entiers positifs, les deux exemples les plus célèbres étant la fonction de Möbius et la fonction indicatrice d'Euler. La fonction de Möbius est définie ainsi :

$$\begin{aligned} &\mu(1) = 1, \\ &\mu(n) = (-1)^k \quad \text{si } a_1 = \cdots = a_k = 1, \\ &\mu(n) = 0 \text{ sinon}, \end{aligned}$$

où n est décomposé en puissances de premiers sous la forme $p_1^{a_1} \dots p_k^{a_k}$. La définition de cette fonction semble étrange, mais elle a de nombreuses applications en théorie des nombres. La fonction indicatrice d'Euler est le nombre d'entiers positifs inférieurs à n qui sont premiers avec n. En tant qu'équation, cela peut s'écrire sous la forme

$$\varphi(n) = \sum_{k=1}^{n} 1,$$

Traduction des pages 36 à 45 de l'article arXiv https://arxiv.org/pdf/1910.01730.
Transcription en LaTeX : Denise Vella-Chemla.

où la somme ne fait intervenir que les k et n premiers entre eux. Si n est supérieur ou égal à 1, nous pouvons également écrire une jolie formule qui relie ces deux fonctions [1].

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

De nombreuses approches ont été suggérées pour tenter de prouver l'hypothèse de Riemann. Par exemple, il y a l'idée d'une preuve spectrale où l'on trouve un opérateur auto-adjoint dont les valeurs propres correspondent magiquement aux zéros non triviaux de la fonction zêta de Riemann. Cette idée a suscité beaucoup d'intérêt lorsqu'elle a été suggérée pour la première fois, mais elle n'a pas encore abouti. La preuve spectrale est distincte de la "théorie spectrale" de la fonction zêta de Riemann, où l'on essaie de déduire des choses sur la fonction zêta en utilisant des formules de sommation impliquant un type différent de fonction analytique [2]. Une autre angle d'attaque intéressant vient de la théorie des matrices aléatoires, où l'on utilise le fait que la fonction zêta de Riemann peut être modélisée par le polynôme caractéristique d'une grande matrice aléatoire hermitienne complexe dont la distribution des valeurs propres est connue sous le nom d'ensemble unitaire gaussien (GUE), et l'on utilise cela pour faire des prédictions sur l'espacement des zéros. En fait, il y a la conjecture de Montgomery sur la corrélation par paires, qui énonce que la corrélation par paires entre les paires de zéros de la fonction zêta est la même que la corrélation par paires entre les paires de valeurs propres de matrices hermitiennes aléatoires.

Il existe des preuves numériques montrant qu'à la limite, la distribution des zéros de la fonction zêta s'approche de la courbe donnée par la distribution des valeurs propres d'une matrice aléatoire GUE, mais en fin de compte, l'approche par matrice aléatoire est un modèle et elle ne peut donc faire que des prédictions intéressantes qui doivent ensuite être prouvées rigoureusement par d'autres moyens. Pour cette raison, il semble extrêmement peu probable que la théorie des matrices aléatoires fournisse une preuve de l'hypothèse de Riemann. Il faut dire que certaines des approches suggérées pour prouver l'hypothèse semblent peu convaincantes, hormis le fait qu'elles puisent de manière passionnante dans plusieurs branches différentes des mathématiques, mais il n'y a aucune preuve qu'avoir simplement une preuve qui relie de multiples domaines des mathématiques rende en quelque sorte la preuve plus convaincante, car on pourrait facilement construire une fausse preuve pour n'importe quoi en puisant des idées dans dix branches différentes des mathématiques.

Un autre problème très important de la liste des problèmes de Hilbert est le dix-neuvième problème : les solutions des problèmes réguliers du calcul des variations sont-elles toujours analytiques ? Ce problème ne semble pas très difficile, mais dans le cas d'intégrales variationnelles régulières, nous nous retrouvons avec une équation d'Euler-Lagrange non linéaire. Le problème a été résolu par De Giorgi en 1957 et Nash indépendamment en 1958 [3]. Le théorème de régularité de De Giorgi énonce que si nous avons $S : \Omega \to \mathbb{R}^{d\times d}$ mesurable et symétrique qui satisfait les estimations suivantes :

$$\mu|v|^2 \leq v^{\mathrm{Tr}} S(x) v \leq M|v|^2,$$

1. Tom Apostol, Introduction to Analytic Number Theory (New York : Springer, 1976).
2. Yoichi Motohashi, Spectral Theory of the Riemann Zeta-Function (Cambridge : Cambridge University Press, 1997).
3. Filip Rindler, Calculus of Variations (Cham, Switzerland : Springer, 2018).

pour des constantes non négatives μ et M, alors u dans l'espace de Sobolev $W^{1,2}(\Omega)$ résout faiblement

$$-\mathrm{div}(S\nabla u) = 0,$$

u est α-Hölder continu pour un certain α entre 0 et 1 dépendant de d et M/μ. Le théorème est appelé théorème de régularité, car il montre la "régularité höldérienne". Combiné avec les estimations standard de Schauder, nous pouvons obtenir le théorème de De Giorgi-Nash-Moser : prenons une intégrale variationnelle régulée $\mathcal{F}$ avec pour intégrande une fonction $f : \mathbb{R}^{d\times d} \to \mathbb{R}$ qui peut être continûment différenciée n fois, alors si u_* est un minimisant de $\mathcal{F}$, alors $u_* \in C^{n-1,\alpha}_{\mathrm{loc}}(\Omega)$ pour un certain α entre 0 et 1. Si l'intégrande f est analytique, alors le minimisant est également analytique. Les méthodes de Nash étaient différentes de celles de De Giorgi, et il convient de mentionner qu'il a été motivé par l'intuition physique en ayant à l'esprit les applications évidentes d'un résultat de régularité aux types de problèmes qui surgissent en physique et en mathématiques appliquées (ce qui faisait presque certainement partie de la motivation de Hilbert pour introduire le problème).

Le dixième problème de Hilbert est plus facile que l'hypothèse de Riemann, mais il reste un problème extrêmement difficile en soi : il demande si l'on peut trouver un algorithme qui indique si une équation diophantienne polynomiale à coefficients dans $\mathbb{Z}$ a une solution dans $\mathbb{Z}$. Matiyasevich a finalement démontré qu'un tel algorithme n'existe pas, en faisant largement appel aux techniques développées par Julia Robinson sur une période de deux décennies de travail sur le problème. Une équation diophantienne est une équation polynomiale qui est résolue sur les entiers. Ce type d'équation a été étudié depuis les temps anciens, mais ce n'est qu'au vingtième siècle qu'une théorie systématique a été développée pour elles. Un exemple d'une telle équation pourrait être :

$$y^2 = x^3 + k,$$

où $k \in \mathbb{Z}$. On cherche alors à voir si l'équation a des solutions $x, y \in \mathbb{Z}$ pour un k donné. Par exemple, dans le cas que nous avons décrit, notre équation n'a pas de solutions lorsque k est de la forme

$$k = (4n-1)^3 - 4m^2,$$

où $m, n \in \mathbb{Z}$ de sorte qu'aucun nombre premier $p \equiv -1 \pmod 4$ ne divise m. Cela peut être prouvé par contradiction en supposant qu'une telle solution existe. Un autre théorème énonce que l'équation diophantienne

$$y^2 = f(x)$$

a un nombre fini de solutions lorsque $f(x)$ est un polynôme de degré supérieur ou égal à 3 avec des valeurs distinctes telles que $f(x) = 0$ et des coefficients dans $\mathbb{Z}$.

L'équation diophantienne la plus célèbre de toutes est

$$x^n + y^n = z^n.$$

Comme nous le savons, on pourrait construire un nombre quelconque de solutions lorsque $n = 2$ ($x = 3, y = 4, z = 5$ est peut-être la première qui vient à l'esprit), mais le dernier théorème de Fermat dit qu'il n'y a pas de solutions en entiers positifs pour $n \geq 3$: cela a finalement été prouvé par Wiles au vingtième siècle en utilisant des techniques auxquelles Fermat n'aurait pas pu avoir accès. Évoquons maintenant les systèmes linéaires d'équations diophantiennes. En général, un

système de congruences linéaires peut n'avoir aucune solution même si les congruences elles-mêmes ont des solutions, mais on peut montrer qu'un système de congruences résolubles peut être résolu simultanément dans une large mesure si et seulement si les modules sont premiers entre eux deux à deux : c'est un théorème élémentaire appelé le théorème des restes chinois. Rappelons que a est congru à b modulo m si m divise $a - b$. Cela s'écrit sous forme d'équation

$$a \equiv b \pmod{m},$$

où m est le module de la congruence. Si vous n'êtes pas familier avec cette notation, pensez à un cadran d'horloge. Si vous commencez au point midi sur l'horloge et avancez de 14 intervalles autour de l'horloge, les 12 premiers intervalles vous ramèneront simplement au départ, de sorte que vous finirez par avancer de 2 intervalles, d'où

$$14 \equiv 2 \pmod{12}.$$

Le théorème des restes chinois énonce que si $m_1, ..., m_r$ sont des entiers positifs qui sont premiers entre eux deux à deux, alors le système de congruences

$$x \equiv b_1 \pmod{m_1}, ..., x \equiv b_r \pmod{m_r}$$

a une solution modulo $m_{12} \cdot ... \cdot m_r$.

Le système de congruences peut également être réécrit comme un système linéaire d'équations diophantiennes :

$$x = a_1 + x_1 n_1, ..., x = a_k + x_k n_k,$$

pour $x, x_i \in \mathbb{Z}$. Vous pourriez résoudre ce système en l'écrivant sous la forme matricielle habituelle

$$Ax = B,$$

et en déterminant la forme normale de Smith de A [4]. Dans le contexte de l'algèbre, vous verrez probablement le théorème énoncé en termes d'isomorphismes d'anneaux, mais c'est une formulation équivalente. Les équations diophantiennes linéaires sont assez faciles à traiter, puisque l'équation de ce type

$$ax + by = c$$

a une solution si et seulement si le plus grand commun diviseur de a et b divise c (cela découle d'un théorème élémentaire sur le pgcd). Écrire des solutions explicites à l'équation ci-dessus relève alors simplement de la recherche de solutions à l'équation

$$ax + by = \text{pgcd}(a, b),$$

ce qui se résume à quelques calculs avec l'algorithme d'Euclide [5].

Le domaine des équations diophantiennes est à distinguer de celui de l'approximation diophantienne, qui est un type de problème distinct qui apparaît en théorie des nombres. La plupart d'entre nous sont familiers avec les nombres rationnels. Les nombres rationnels sont des fractions $r = p/q$, où

4. Tom Apostol, Introduction to Analytic Number Theory (New York : Springer, 1976).
5. Martin Erickson et Anthony Vazzana, Introduction to Number Theory (New York : Chapman Hall, 2008).

p et q sont des entiers positifs ou négatifs. $\mathbb{Q}$ forme un sous-ensemble infini dénombrable de $\mathbb{R}$, et un nombre réel qui n'est pas un nombre rationnel est appelé nombre irrationnel (presque chaque élément de $\mathbb{R}$ est irrationnel, et il y a des nombres irrationnels célèbres comme π et e). La question qui se pose à un théoricien des nombres est exactement de savoir dans quelle mesure les nombres réels peuvent être approchés par des nombres rationnels. Dans le cas de la dimension 1, il existe un lien fort avec les développements en fractions continues. Si nous commençons par un nombre irrationnel α, alors il y aura un nombre infini d'entiers premiers entre eux m et n tels que

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}.$$

Une autre façon de le voir est que αn est dense (mod 1) lorsque α est irrationnel. Pour un nombre irrationnel α et un entier positif q, le vecteur

$$(x_1, ..., x_1) = (\alpha \bmod 1, ..., q\alpha \bmod 1)$$

possède un élément qui est le plus proche de 0 mod 1. La divergence de la liste αn (mod 1) est contrôlée par le développement en fractions continues de α. Une chose que nous pouvons dire est que si $\alpha \in \mathbb{R}$ est compris entre 0 et 1/2 et $p, q \in \mathbb{Z}$ de sorte que $(0/1, p_1/q_1, p_2/q_2, ...)$ sont les limites de α et de plus si $q > q_1$ et $|\alpha - p/q| \leq 1/2q^2$, alors p/q est une limite exprimée comme une fraction continue du nombre réel α [6].

Bien qu'il existe un algorithme pour déterminer si une équation diophantienne est résoluble ou non, les travaux de Julia Robinson ont fourni des résultats utiles : par exemple, le fait qu'un ensemble diophantien peut formellement être presque n'importe quoi. Rappelons que nous pouvons écrire un système de m équations diophantiennes. Ce système n'aura une solution que si la somme des carrés de chacune des équations individuelles

$$D_1(x_1, ..., x_n)^2 + \cdots + D_m(x_1, ..., x_n)^2 = 0$$

a une solution, de sorte que l'on peut toujours convertir un problème de résolution d'un système d'équations diophantiennes en un problème de résolution d'une seule équation diophantienne. Nous disons qu'un ensemble S de m-uplets est diophantien s'il existe une famille d'équations diophantiennes avec des paramètres $\alpha_1, ..., \alpha_m$ et des inconnues $x_1, ..., x_n$

$$D(\alpha_1, ..., \alpha_m, x_1, ..., x_n) = 0$$

qui a une solution $x_1, ..., x_n$ si et seulement si le m-uplet $(\alpha_1, ..., \alpha_m)$ est contenu dans S. Dans le cas où $m = 1$, cela se réduit au fait que l'ensemble des entiers non négatifs est un ensemble diophantien si et seulement si "il y a une équation diophantienne $D = 0$ qui a une solution si et seulement si le paramètre α appartient à cet ensemble". Un ensemble d'entiers positifs est diophantien si et seulement s'il est l'ensemble des valeurs positives d'un polynôme qui a des valeurs entières non négatives des variables. L'ensemble de tous les nombres pairs est un ensemble diophantien parce qu'il y a une famille diophantienne résoluble

$$a - 2x = 0.$$

6. Doug Hensley, Continued Fractions (Singapore : World Scientific Publishing, 2006).

L'ensemble de tous les nombres impairs est également diophantien (il suffit d'ajouter 1 à la famille).

$$a - (2x + 1) = 0.$$

Les nombres de Fibonacci forment un ensemble diophantien parce qu'il existe une représentation diophantienne

$$y^2 - xy - x^2 = \mp 1.$$

Cette représentation est en fait utilisée dans la preuve d'indécidabilité pour le dixième problème de Hilbert. La classe de tous les ensembles diophantiens est fermée sous les opérateurs d'intersection et d'union.

La question globale à laquelle nous souhaitons répondre est de savoir s'il existe un algorithme qui peut nous dire si une équation diophantienne est résoluble, nous devons donc être clairs sur ce qu'est un algorithme et ce que calcule un algorithme. Pour notre objectif, il suffit de penser à un algorithme comme à une procédure que l'on exécute pour engendrer des nombres positifs. Vous pouvez vérifier que l'algorithme d'Euclide est en fait un algorithme lorsque vous suivez cette définition : l'algorithme peut être utilisé par n'importe qui, indépendamment de la quantité d'ingéniosité requise pour le découvrir : vous y mettez l'entrée, et vous obtenez un résultat. Turing a imaginé de manière célèbre un ordinateur appelé la machine de Turing qui pouvait calculer le résultat de l'exécution de n'importe quel algorithme et il y a une hypothèse qui énonce (de manière informelle) que tout algorithme calculable peut être calculé par une machine de Turing [7].

Un ensemble de nombres naturels qui peut être produit via des calculs effectués avec une machine de Turing est appelé "ensemble récursivement énumérable". Dans cette catégorie, on peut imaginer un ensemble tel que la machine de Turing peut dire qu'un nombre naturel donné est un membre de cet ensemble. Si cela peut être fait pour tous les nombres naturels, alors l'ensemble est dit récursif. Un ensemble de nombres naturels est récursif si et seulement si l'ensemble et son complément sont récursivement énumérables. Il semble difficile de penser à un ensemble qui n'est pas récursivement énumérable, mais cela se produit lorsque l'on tente de déterminer si un programme peut continuer à tourner pendant une infinité de temps (un programme étant un code P avec ses données d). On a démontré le résultat important que chaque ensemble diophantien est récursivement énumérable : on peut simplement écrire un algorithme qui prend une famille diophantienne et parcourt tous les n-uplets pour voir s'ils en sont des solutions. On peut représenter un ensemble d'entiers non négatifs S avec une formule arithmétique $\mathfrak{F}$: on dit que l'ensemble S est représenté par une formule avec une variable a s'il y a une équivalence $a \in S \iff \mathfrak{F}$. Gödel a montré que tout ensemble récursivement énumérable est représenté par une formule arithmétique d'une certaine sorte, mais Julia Robinson et Matiyasevich ont considérablement amélioré ce résultat en montrant que tous les ensembles récursivement énumérables d'entiers non négatifs peuvent être représentés par deux types de formule arithmétique qui peuvent être écrits explicitement et qui ne contiennent que 3 quantificateurs [8] :

$$\exists b\, \exists c\, \& \, \exists d\, [P_i(a, b, c) < D_i(a, b, c)d < Q_i(a, b, c)],$$

$$\exists b\, \exists c\, \forall f\, [f \leq F(a, b, c) \implies W(a, b, c, f) > 0].$$

7. Martin Erickson et Anthony Vazzana, Introduction to Number Theory (New York : Chapman Hall, 2008).

8. Yuri Matiyasevich et Julia Robinson, *Two universal 3-quantifier representations of recursively enumerable sets*, Teoriya Algorifmov i Matematicheskaya Logika, Vychislitel'nyi Tsentr Akademii Nauk SSR, 1974, 112–123.

Nous sommes maintenant en mesure d'esquisser les raisons pour lesquelles il y a une solution négative pour le dixième problème. Julia Robinson, Matiyasevich et d'autres avaient montré que chaque ensemble récursivement énumérable est diophantien. Cependant, nous avons déjà dit que chaque ensemble diophantien est récursivement énumérable. Puisque la correspondance va dans les deux sens, l'ensemble des ensembles diophantiens et l'ensemble des ensembles récursivement énumérables sont le même ensemble. Les ensembles récursifs forment une sous-classe des ensembles récursivement énumérables, alors prenons un ensemble d'entiers non négatifs S qui est récursivement énumérable mais pas récursif. Puisque S est aussi diophantien, il a une représentation via une famille diophantienne

$$D(a, x_1, ..., x_n) = 0.$$

Si le dixième problème pouvait être résolu, alors le problème de décision serait résolu pour cette famille. C'est une contradiction, donc le dixième problème ne peut pas être résolu. L'étape clé, alors, est de prouver que tous les ensembles récursivement énumérables sont diophantiens. Davis, Putnam et Julia Robinson ont commencé par prouver d'abord que tous les ensembles récursivement énumérables sont exponentiels diophantiens [9]. Tout ensemble diophantien a une fonction diophantienne associée : c'est simplement une fonction telle que le graphe de la fonction f, i.e. $\{(m, n) : n = f(m)\}$, est un ensemble diophantien. On peut considérer comme exemple d'une fonction diophantienne la fonction factorielle. On peut définir un ensemble diophantien exponentiel comme un ensemble dont la fonction de définition est construite à partir de polynômes et d'une fonction exponentielle. Il n'est pas trop difficile de prouver que tous les ensembles diophantiens exponentiels sont diophantiens si la fonction exponentielle elle-même est diophantienne. On savait déjà que la fonction exponentielle est diophantienne puisqu'on pouvait exhiber une fonction diophantienne qui *croît* exponentiellement. Matiyasevich a prouvé qu'une telle fonction diophantienne existe sous la forme d'une fonction $n = f_{2m}$, où f_{2m} est le $2m$-ième nombre de Fibonacci (rappelons que les nombres de Fibonacci forment une suite à croissance exponentielle).

Il existe cependant des preuves plus simples qui utilisent des solutions à une version de l'équation de Pell

$$x^2 - (a^2 - 1)y^2 = 1.$$

L'équation de Pell originale est

$$x^2 - dy^2 = 1.$$

C'est une équation diophantienne, donc étant donné un d, une solution est une paire d'entiers non négatifs. En fait, une autre preuve modifie encore l'équation de Pell et considère l'équation

$$x^2 - \lambda xy + y^2 = 1.$$

Prenons $\lambda \geq 2$. On peut prouver qu'une paire d'entiers satisfait l'équation ci-dessus si et seulement si $(x, y) = (a_n, a_{n+1})$ ou $(x, y) = (a_{n+1}, a_n)$ pour une suite $\{a_n\}$ définie par la relation de récurrence

$$a_n = \lambda a_{n-1} - a_{n-2}, \quad n \geq 2,$$

$$a_0 = 0, a_1 = 1.$$

9. Martin Davis, Hilary Putnam et Julia Robinson, *The decision problem for exponential Diophantine equations*, Annals of Mathematics, 74(3), 425 – 436 (1961).

Rappelons qu'une relation de récurrence définit une suite une fois qu'une ou plusieurs valeurs initiales ont été spécifiées. Dans le cas des nombres de Fibonacci, la relation de récurrence est

$$f_n = f_{n-1} + f_{n-2},$$

de sorte que deux valeurs initiales doivent être spécifiées. On peut généralement repérer la relation par inspection. Par exemple, si nous avons une suite de termes

$$a_1 = -\frac{1}{4}, a_2 = \frac{1}{36}, a_3 = -\frac{1}{576}, a_4 = \frac{1}{14400}, ...,$$

alors la relation de récurrence est

$$a_n = -\frac{a_{n-1}}{(n+1)^2}.$$

Nous nous intéressons particulièrement à la suite $\{a_n(\lambda)\}$ qui satisfait une relation de récurrence

$$a_n(\lambda) = \lambda a_{n-1}(\lambda) - a_{n-2}(\lambda), \quad n \geq 2,$$

$$a_0(\lambda) = 0, a_1(\lambda) = 1.$$

Les termes consécutifs de cette suite sont premiers entre eux. On peut montrer que la fonction $a = a_b(\lambda)$ est diophantienne lorsque $\lambda \geq 4$ et à partir de là, on peut prouver que la fonction exponentielle $a = \lambda^b$ est diophantienne. On commence par les inégalités

$$(\lambda - 1)^{n-1} \leq a_n(\lambda) \leq \lambda^{n-1}, n \geq 1.$$

On peut obtenir une borne supérieure sur le quotient

$$\frac{a_{b+1}(\lambda x)}{a_{b+1}(x+1)} \leq \frac{(\lambda x)^b}{x^b} = \lambda^b,$$

ainsi qu'une borne inférieure

$$\frac{a_{b+1}(\lambda x)}{a_{b+1}(x+1)} \geq \frac{(\lambda x - 1)^b}{(x+1)^b} > \lambda^b - 1.$$

On peut ensuite écrire la fonction exponentielle en termes de la fonction partie entière (c'est-à-dire la fonction qui donne le plus petit entier qui est supérieur ou égal à la quantité entre crochets) de ce quotient :

$$\lambda^b = \left\lfloor \frac{a_{b+1}(\lambda x)}{a_{b+1}(x+1)} \right\rfloor, x > 2ab_{b+1}(\lambda + 1) - 1.$$

Il est possible de démontrer que la fonction partie entière d'un quotient est diophantienne. Cela prouve que la fonction exponentielle est diophantienne, ce qui prouve que le dixième problème de Hilbert est indécidable [10].

Mentionnons maintenant les contributions de Julia Robinson à la théorie des jeux. Les deux chercheurs les plus connus dans ce domaine sont Nash et von Neumann (en fait, la théorie des jeux moderne n'a pas vraiment existé jusqu'aux travaux de von Neumann). Par essence, la théorie des

10. Martin Erickson et Anthony Vazzana, Introduction to Number Theory (New York : Chapman et Hall, 2008).

jeux étudie les phénomènes qui sont observés lors d'interactions entre des décideurs rationnels (ou plutôt, elle étudie des modèles mathématiques simplifiés de ces interactions). Les modèles mathématiques et l'application des mathématiques aux situations du monde réel ne se limitent certainement pas à la physique, et apparaissent fortement dans la finance et l'économie. Nous supposons non seulement que les décideurs sont rationnels, mais qu'ils utilisent une sorte de stratégie qui prend en compte le comportement attendu de tout autre décideur dans le jeu. Un jeu que nous connaissons tous (ou une certaine variante) est le dilemme du prisonnier. Imaginons que deux suspects soient placés dans des cellules de prison séparées, sans aucun moyen de communiquer ou d'influencer l'autre. S'ils avouent tous les deux le crime, ils recevront tous les deux une peine de trois ans de prison. Si l'un d'eux avoue, il s'en tirera libre, et l'autre recevra une peine de quatre ans. Si aucun d'eux n'avoue, ils passeront tous les deux seulement un an en prison.

C'est un scénario intéressant, car le résultat global pour les deux prisonniers serait intéressant si aucun d'eux ne dit rien, mais il y a une incitation à prendre un risque et à avouer à la place. En fait, quoi que fasse l'autre prisonnier, il est toujours préférable d'avouer plutôt que de ne rien dire. Cela signifie que ce jeu n'a qu'un seul équilibre de Nash, où les deux joueurs avouent. Dans le cas où nous jouons à un jeu où deux personnes souhaitent aller ensemble dans un centre commercial mais l'un veut aller dans un magasin et l'autre préfère un autre magasin, il y a deux équilibres de Nash possibles. L'équilibre de Nash est une sorte d'état stationnaire stratégique dans lequel un jeu finit par se stabiliser. Mathématiquement, un jeu stratégique est un triplet $\langle N, (A_i), (\geq_i)\rangle$ où N est l'ensemble des joueurs, A_i est l'ensemble des actions qui sont disponibles pour chaque joueur i et $\geq_i$ est une relation de préférence binaire sur l'ensemble $A = \times_{j\in N} A_j$ pour chaque joueur. Une collection de valeurs d'une variable, une pour chaque joueur, est appelée un profil. Un équilibre de Nash d'un jeu est un profil a^* dans l'ensemble A tel que pour chaque joueur, la relation suivante est satisfaite :

$$(a^*_{-i}, a^*_i) \geq_i (a^*_{-i}, a_i) \text{ pour tout } a_i \in A_i.$$

Pour que le profil a^* soit un équilibre de Nash, il faut qu'aucun joueur n'ait une action qui donne un résultat qu'il ou elle préfère au résultat qu'il ou elle obtient lorsqu'il ou elle choisit a^*_i, étant donné que les autres joueurs choisissent leurs actions d'équilibre respectives a^*_{-i}. Tout jeu stratégique n'a pas d'équilibre de Nash, et il est intéressant d'étudier les conditions sous lesquelles nous avons des équilibres pour un jeu. Bien sûr, nous ne pouvons pas dire grand-chose si nous essayons de parler de tous les jeux en général et nous devons donc faire une restriction (tous les jeux compétitifs à deux joueurs, par exemple)[11]. Il est possible d'avoir un certain type de processus d'ajustement qui conduit à un équilibre de Nash. Un exemple d'un tel processus est appelé jeu fictif, où un joueur choisit toujours une meilleure réponse à la fréquence des actions passées des autres joueurs pendant le jeu. Julia Robinson a prouvé que dans tout jeu strictement compétitif, le processus de jeu fictif converge toujours vers un équilibre de stratégie mixte, où un équilibre de ce type est un profil de stratégie mixte a^* avec la propriété que pour chaque joueur, chaque action dans le support de a^*_i est une meilleure réponse à a^*_{-i}. Informellement, une stratégie mixte est une stratégie telle que les choix sont faits selon des règles probabilistes. On peut prouver que tout jeu stratégique fini a un équilibre de Nash en stratégie mixte[12].

11. Martin Osborne et Ariel Rubinstein, A Course in Game Theory (Cambridge, Massachusetts : MIT Press, 1994).

12. Julia Robinson, *An iterative method of solving a game*, Annals of Mathematics 54, 296 – 301 (1951).