Les jeux diophantiens

Michel Lafond(*)

Cet article explore le lien très étroit qui existe entre Jeux et Mathématiques.

I. Introduction.

Ce qui m'a mis sur la piste des jeux diophantiens est le livre extraordinaire :

GÖDEL, ESCHER, BACH. Les Brins d'une Guirlande Éternelle.
de Douglas HOFSTADTER, *InterÉditions*.

Ce livre est encore sur certains rayons plus de 20 ans après sa publication ! Ce n'est pas vraiment un livre de maths bien que l'auteur démontre au passage le théorème d'incomplétude de Gödel d'une manière accessible à tous !
Dans le chapitre VIII : « Un système explosif : la TNT », l'auteur expose un système (TNT = Théorie des Nombres Typographiques) permettant d'écrire tous les énoncés de l'arithmétique usuelle des nombres entiers à l'aide d'un nombre réduit de symboles. En gros les deux quantificateurs : $\forall$, $\exists$, les connecteurs logiques usuels $\neg$ pour la négation, $\wedge$ pour la conjonction, $\vee$ pour la disjonction, $\Rightarrow$ pour l'implication, le symbole relationnel =, les parenthèses ouverte et fermée, un alphabet pour désigner les variables (uniquement des entiers naturels), et les constantes 0, 1, 2, etc.
Dans l'arithmétique (de Peano), on a une addition +, une multiplication × mais <u>pas d'exponentiation</u>. C'est très important pour la suite.

On traduit ainsi dans le langage de la TNT :
« n est pair » par $\exists k\ n = 2 \times k$ [le symbole $\in$ est inconnu].

« 2 n'est pas un carré » par $\forall a\ \neg(a \times a = 2)$ [a^2 est inconnu sauf définition préalable].

« p est premier » par $\forall a \forall b\ \big((\exists c\ \ a = 2 + c) \wedge (\exists d\ \ b = 2 + d)\big) \Rightarrow \neg(p = a \times b)$.

Cet exercice de traduction est déjà amusant en soi (essayez par exemple de traduire : « Il y a une infinité de nombres premiers »), mais là où ça devient encore plus intéressant, c'est lorsqu'on aborde l'exponentiation.

<u>Comment écrire dans la TNT « x est une puissance de 2 » ?</u>

Il faut peu de temps pour s'apercevoir qu'on élimine le terme gênant « puissance » en disant : x est une puissance de 2 si et seulement si tout diviseur de x autre que 1 est pair. Après quoi on obtient l'écriture :

$$\forall d\ \ (\exists k\ \ x = k \times d) \Rightarrow (d = 1) \vee (\exists l\ \ d = 2 \times l).$$

(*) mlafond001@yahoo.fr

Et voilà le plus beau. Douglas HOFSTADTER demande dans le chapitre VIII :

Traduire dans la TNT la phrase « x est une puissance de 10 » ?

Et il ajoute « Pour écrire cette phrase dans la TNT il faut curieusement beaucoup d'astuce. Je vous conseille de ne vous y coller que si vous êtes prêt à y passer des semaines et si vous avez des connaissances assez poussées de la théorie des nombres ».
En lisant ceci, je me suis dit : ca tombe bien, j'ai du temps et des connaissances en théorie des nombres.
Bien entendu, les semaines se sont écoulées sans succès. D'où je déduis que mes connaissances ne sont pas assez poussées.
Plusieurs années après, je tombe sur le livre :

Le dixième problème de Hilbert. Son indécidabilité.
de Youri MATIIASSEVITCH, *Masson*.

Dans ce livre Youri MATIIASSEVITCH prouve que « L'exponentiation est diophantienne », c'est-à-dire en gros qu'on peut traduire la phrase « x est une puissance de y » dans la TNT. C'est très intéressant, l'auteur détaillant avec humour sa démarche avec tous ses aléas dans sa collaboration avec Julia Robinson.

Le problème de Douglas HOFSTADTER : traduire dans la TNT « x est une puissance de 10 » était résolu ipso facto. Ce qui me rassure, c'est que Youri MATIIASSEVITCH y a passé beaucoup plus que quelques semaines !

Enfin, c'est dans ce même livre que Youri MATIIASSEVITCH décrit au chapitre 10 les « Jeux diophantiens » qui ne sont qu'un aspect des représentations diophantiennes au cœur de son ouvrage.

II. Le lien entre jeux diophantiens et énoncés de l'arithmétique.

En fait, il s'agit de beaucoup plus qu'un lien, puisque nous allons voir que dans le domaine de l'arithmétique des nombres entiers naturels, à de très nombreux énoncés comme par exemple

E : « Il existe une infinité de nombres premiers »,

on peut associer un jeu à deux joueurs A, B dans lequel A et B jouent à tour de rôle, A jouant le premier, de telle sorte que :

> Affirmer que E est vrai équivaut à affirmer qu'il existe une stratégie gagnante pour le joueur A (ou qu'il existe une stratégie gagnante pour le joueur B.)

En ce qui concerne l'énoncé E « Il existe une infinité de nombres premiers » mentionné plus haut, une partie est « jouée » dans le paragraphe V, et le lien entre l'énoncé E et le jeu J associé est décrit en détail dans le paragraphe VI. Nous verrons que affirmer la vérité de E équivaut à dire qu'il existe une stratégie gagnante pour le joueur A.

Avant de passer aux généralités, prenons deux exemples :

Exemple 1 :
Considérons le polynôme $J_1 = a_1 + a_2 - b_1b_2$ dont les quatre variables sont des entiers naturels.
À ce polynôme on va associer un jeu à deux personnes A, B de la manière suivante :

A choisit comme il veut un entier naturel a_1 ; il en informe B.
B choisit comme il veut un entier naturel b_1 ; il en informe A.
A choisit comme il veut un entier naturel a_2 ; il en informe B.
B choisit comme il veut un entier naturel b_2 ; il en informe A.

De deux choses l'une :
Ou bien la quantité $a_1 + a_2 - b_1b_2$ est non nulle et A est déclaré gagnant, ou bien cette quantité est nulle et B est déclaré gagnant. [On aurait pu prendre la règle inverse].
La question immédiate est : le « NUL » étant impossible, qui est gagnant à ce jeu ?
D'après la règle, B pour gagner doit faire en sorte que $b_1b_2 = a_1 + a_2$.
Il joue le dernier coup b_2 mais A peut rendre l'entier $a_1 + a_2$ arbitraire.
B doit donc être en mesure de factoriser l'entier $a_1 + a_2$ arbitraire, et pour cela il lui suffit de choisir $b_1 = 1$ puis $b_2 = a_1 + a_2$.
B n'a d'ailleurs pas le choix de sa stratégie, car s'il joue $b_1 \neq 1$, A qui connaît b_1 jouera a_2 pour rendre $a_1 + a_2$ non multiple de b_1, et quelle que soit la réponse b_2 de B, $a_1 + a_2 - b_1b_2$ sera non multiple de b_1 donc non nul.
En ce qui concerne le « jeu » $J_1 = a_1 + a_2 - b_1b_2$, on dira que son statut est « gagnant pour B ».
L'analyse précédente montre que l'affirmation : « J_1 est gagnant pour B » implique que le théorème (E_1) : Pour tout entier naturel n, on peut trouver deux entiers naturels x et y tels que $x \cdot y = n$ est vrai.
Par l'intermédiaire d'un polynôme, on est donc passé d'un JEU à un ÉNONCÉ arithmétique.

Inversement, à partir d'un ÉNONCÉ arithmétique (E), on peut souvent construire un polynôme JEU de telle sorte que affirmer que (E) est vrai c'est affirmer que le jeu est gagnant pour A (ou pour B).

Exemple 2 :

Soit l'énoncé (E_2) dû à Lebesgue : l'équation $x^2 - y^3 = 7$ n'a pas de solution dans $\mathbb{N}$.
En changeant les variables, considérons le polynôme $J_2 = b_1^2 - b_2^3 - a_1 - a_2$.

Il est clair que le joueur A, (s'il connaît le résultat de Lebesgue !), pourra choisir comme stratégie (entre autres) $a_1 = 7$ puis $a_2 = 0$ mettant B dans l'impossibilité d'annuler J_2 donc de gagner.
Cette fois, par l'intermédiaire d'un polynôme, on est passé d'un ÉNONCÉ arithmétique à un JEU de telle sorte que la vérité de (E_2) implique que le jeu est gagnant pour A.

Passons maintenant aux définitions générales.

III. Qu'est-ce qu'un jeu diophantien ?

C'est un jeu qui se joue à deux joueurs A et B.
La règle est tout entière contenue dans la donnée d'un polynôme J que les deux joueurs connaissent.
Ce polynôme a ses variables parmi un ensemble fini V que nous désignerons systématiquement par : $V = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n\}$.
On peut qualifier n de « Taille du jeu ».

Le domaine des variables est l'ensemble $\mathbb{N}$ des entiers naturels. D'où l'adjectif diophantien.
Les coefficients du polynôme sont les entiers relatifs.
Dans la TNT, il n'y a pas de soustraction, mais on a l'équivalence entre $x = a - b$ et $x + b = a$. Donc l'addition, la soustraction et la multiplication des variables sont autorisées. De plus, on admettra bien sûr les écritures comme b_1^3 pour $b_1 \times b_1 \times b_1$.

Par contre, les variables en exposant sont interdites, ainsi $b_1^{a_3}$ est interdit.

Exemples de polynômes « jeux » qui seront utilisés dans la suite :

$$P = b_1 + a_2 - 2b_2 - 2b_3 - b_2b_3 - 4,$$

$$Q_1 = (1 + b_1)^3 + (1 - b_2)^3 - b_3^3,$$

$$Q_2 = a_1 + b_1,$$

$$Q_3 = 23.$$

Remarques :

La taille n du polynôme P ci-dessus vaut 3 mais seules les variables $\{b_1, a_2, b_2, b_3\}$ sont utilisées.
a_1 et a_3 sont absentes, mais on peut parfaitement les réintroduire sans changer le jeu en leur affectant un coefficient nul. P deviendrait ainsi

$$P = b_1 + a_2 - 2b_2 - 2b_3 - b_2b_3 - 4 + 0(a_1 + a_3).$$

Ainsi dans la suite, par commodité, on ne considèrera que des polynômes ayant pour variables un ensemble tel que $V = \{a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n\}$. Par contre les variables affectées d'un coefficient nul, donc sans effet, seront souvent omises dans l'écriture pour plus de lisibilité.

Dans Q_3, il n'y a aucune variable. Q_3 est un polynôme constant. On peut admettre que sa taille est $n = 0$.

IV. Comment joue t-on à un jeu diophantien ?

C'est extrêmement simple. Le polynôme J du jeu étant donné :
A commence et annonce pour la variable a_1 un entier naturel de son choix qu'on désignera encore par abus par a_1. Le choix est public, c'est-à-dire que B en a immédiatement connaissance.
Bien entendu, si la variable a_1 ne figure pas dans J, ou si elle a un coefficient nul, le choix de A est sans importance et tout se passe comme si A passait son tour.

(Signalons que dans de nombreux jeux il est possible de passer son tour : une enchère au bridge est « Je passe » ; au go à tout moment un joueur peut passer…)
Ensuite c'est à B de jouer. Il choisit pour la variable b_1 un entier naturel qu'on désignera encore par b_1.
Le choix est public, c'est-à-dire que A en a immédiatement connaissance.
Si la variable b_1 ne figure pas dans J, ou si elle a un coefficient nul, B choisira n'importe quel entier ou passera son tour.
(Il peut même se faire que ni a_1 ni b_1 ne figurent dans J. Mais dans ce cas tout se passe comme si A et B passaient leur premier tour. Ce cas est un peu ridicule et il suffit de renuméroter les variables pour l'éviter.)
Ensuite, A choisit pour la variable a_2 un entier naturel a_2 ou passe son tour si a_2 est absente de J.
Et ainsi de suite comme dans tous les jeux, tant qu'il y a des variables dans V.
Un jeu diophantien de taille n comporte donc n tours, et dans le cas exceptionnel où $n = 0$, le jeu est terminé avant d'avoir commencé !
Les indices servant de numéros aux variables sont très importants puisqu'ils imposent l'ordre des choix.

V. Qui gagne à un jeu diophantien ?

C'est encore plus simple : à l'issue des n tours, quand chacun a choisi ses n variables, de deux choses l'une : ou bien la valeur $Z = J(a_1, b_1, a_2, b_2, a_3, b_3, \ldots, a_n, b_n)$ est non nulle et c'est A qui gagne, ou bien $Z = 0$ et c'est B qui gagne.
Il n'y aura donc jamais « nulle ».

Il suffit de retenir ceci : **B doit annuler pour gagner**.

Voyons deux exemples de parties :

• Le jeu $Q_2 = a_1 + b_1$ cité plus haut.
Pour gagner B doit faire en sorte d'annuler $a_1 + b_1$. Si A a un peu de jugeote, il jouera a_1 strictement positif, et B perdra puisqu'il ne pourra pas annuler Q_2.
On dira que le statut de Q_2 est « gagnant pour A » ou plus brièvement que A gagne.

• Le jeu $P = b_1 + a_2 - 2b_2 - 2b_3 - b_2 b_3 - 4$ associé à l'énoncé E « Il existe une infinité de nombres premiers » du début. Le paragraphe VI explique la provenance de ce polynôme.
Ici, $V = \{a_1, b_1, a_2, b_2, a_3, b_3\}$. Donc P se joue en 3 tours.

Considérons coup par coup la partie suivante du jeu P :
A joue $a_1 = 0$ (ou n'importe quoi puisque a_1 est absente des variables de P).
B joue $b_1 = 13$.
A joue $a_2 = 17$.
B joue $b_2 = 9$.
A joue n'importe quoi pour a_3 (qui est absente de P) ou passe son tour.
B doit jouer le dernier coup b_3 et d'après la règle, il gagnera si

$$Z = P(0, 13, 17, 9, 0, b3) = 13 + 17 - 2 \times 9 - 2\, b_3 - 9\, b_3 - 4 = 0.$$

C'est malheureusement impossible car Z = 8 − 11b_3 et on joue dans ℕ. B a perdu cette partie.

B pouvait-il « gagner à coup sûr » en jouant différemment ? [La réponse est dans le paragraphe VI].
Il faut d'abord définir ce qu'on entend par « gagner à coup sûr » et c'est le bon moment pour définir ce qu'est une « stratégie gagnante » pour B (ou pour A).

> Dire que A a une stratégie gagnante au jeu J(a_1, b_1, a_2, b_2, a_3, b_3, …, a_n, b_n) signifie précisément ceci :
> Il existe un coup a_1 tel que quelle que soit la réponse b_1 il existe un coup a_2 tel que quelle que soit la réponse b_2 il existe un coup a_3 tel que quelle que soit la réponse b_3, … il existe un coup a_n tel que quelle que soit la réponse b_n A gagne.
> Cela s'écrit
>
> $$\exists a_1\ \forall b_1\ \exists a_2\ \forall b_2\ \exists a_3\ \forall b_3 \ldots \exists a_n\ \forall b_n\quad \mathrm{J}\left(a_1, b_1, a_2, b_2, \ldots a_n, b_n\right) \neq 0. \qquad (1)$$

Rappelons que les écritures du genre $\forall x \in \mathrm{E}$ bien que très utilisées sont parfois abusives comme ici dans le cadre strict de l'arithmétique, car le symbole $\in$ fait partie de la théorie des ensembles, pas de l'arithmétique. Voir à ce sujet les écritures du paragraphe I.

Si (1) est vraie, A a une stratégie gagnante, c'est parfait pour lui, et il jouera les coups a_1, a_2, …, a_n dont l'existence est garantie par (1).

Supposons maintenant que A n'a pas de stratégie gagnante, c'est-à-dire que (1) est fausse.
En se souvenant qu'en logique, le contraire de « tous les chats sont gris » est « il y a un chat non gris », et le contraire de « il y a un méchant » est « tout le monde est gentil », si $\neg$ désigne la négation, et P une proposition, alors la négation de $\forall a\, \mathrm{P}$ est $\exists a \neg \mathrm{P}$ et la négation de $\exists a\, \mathrm{P}$ est $\forall a \neg \mathrm{P}$.
Puisque (1) est fausse, la négation de (1) est vraie et s'écrit donc :

$$\forall a_1\ \exists b_1\ \forall a_2\ \exists b_2\ \forall a_3\ \exists b_3 \ldots \forall a_n\ \exists b_n\quad \neg\, \mathrm{J}\left(a_1, b_1, a_2, b_2, \ldots a_n, b_n\right) \neq 0$$

ou encore

$$\forall a_1\ \exists b_1\ \forall a_2\ \exists b_2\ \forall a_3\ \exists b_3 \ldots \forall a_n\ \exists b_n\quad \mathrm{J}\left(a_1, b_1, a_2, b_2, \ldots a_n, b_n\right) = 0. \qquad (2)$$

Si on décortique (2), la traduction est exactement celle-ci :
Quel que soit le coup a_1 il existe une réponse b_1 telle que quel que soit le coup a_2 il existe une réponse b_2 telle que quel que soit le coup a_3 il existe une réponse b_3 … quel que soit le coup a_n il existe une réponse b_n telle que B gagne. En résumé : B a une stratégie gagnante !

Ainsi, pour tout jeu diophantien J :
Ou bien il existe une stratégie gagnante pour A ou bien il existe une stratégie gagnante pour B.

Ce n'était pas évident *a priori*, d'ailleurs ce résultat ne s'applique pas aux échecs (entre autres), car le contraire de « A fait mat » n'est pas « B fait mat » !

VI. Étude complète du jeu $\mathrm{P} = b_1 + a_2 - 2b_1 - 2b_3 - b_2 b_3 - 4$.

On va prouver qu'à ce jeu, c'est A qui a une stratégie gagnante, et par la même occasion, on va voir que l'affirmation

« A a une stratégie gagnante au jeu P »

est logiquement équivalente à la vérité de l'énoncé E :

« Il y a une infinité de nombres premiers ».

En effet, P peut s'écrire $\mathrm{P} = b_1 + a_2 - (b_2 + 2)(b_3 + 2) + 0 \cdot (a_1 + a_3)$.

A joue a_1 [ce qui n'aura aucun effet sur le résultat final].
B joue b_1.
A se met alors à la recherche d'un nombre premier $p \geq b_1$. Il en existe, et même une infinité.

A joue alors $a_2 = p - b_1$ qui est bien dans $\mathbb{N}$.
B joue b_2.
A joue a_3 [ce qui n'aura aucun effet sur le résultat final à cause du facteur 0 de a_3].
Hélas pour B, il est impossible que le résultat

$$\mathrm{Z} = b_1 + a_2 - (b_2 + 2)(b_3 + 2) + 0 \cdot (a_1 + a_3)$$

soit nul, puisque $\mathrm{Z} = p - (b_2 + 2)(b_3 + 2)$ et si on avait $\mathrm{Z} = 0$, p aurait deux diviseurs plus grands que 1, ce qui est en contradiction avec la primalité de p.
A gagne systématiquement au jeu P, et tout ce qu'il doit faire pour cela est de trouver, immédiatement après le coup b_1 de B, un nombre premier p supérieur ou égal à b_1.
On voit bien ici que l'existence d'une stratégie gagnante pour A est très exactement équivalente au fait qu'il y a des nombres premiers arbitrairement grands.

Si, dans un univers imaginaire, les nombres premiers étaient majorés par M, B aurait une stratégie gagnante consistant à choisir $b_1 = \mathrm{M} + 1$ par exemple. Alors $\mathrm{C} = b_1 + a_2 = \mathrm{M} + 1 + a_2$ est strictement plus grand que M, donc composé (dans notre univers imaginaire).
De plus $\mathrm{C} = \mathrm{M} + 1 + a_2$ étant plus grand que 1, on peut écrire $\mathrm{C} = \mathrm{X\,Y}$ avec X et Y au moins égaux à 2.
B n'aurait plus qu'à jouer pour ses deux derniers coups : $b_2 = \mathrm{X} - 2$ et $b_3 = \mathrm{Y} - 2$.
Alors, $\mathrm{Z} = \mathrm{C} - \mathrm{X\,Y} = 0$. B annule, il gagne !

<u>Attention</u> : Lorsqu'on dit que tout ce que A doit faire pour gagner au jeu P est de trouver un nombre premier p supérieur à b_1, cela risque d'être difficile dans notre univers, car si B, futé, choisit disons $b_1 = 10^{100\,000\,000}$, A devra trouver un nombre premier ayant plus de 100 millions de chiffres. Hélas, le plus grand nombre premier connu en novembre 2010 a un peu moins de 13 millions de chiffres [c'est le nombre de Mersenne $2^{43\,112\,609} - 1$], et il faut espérer que A n'a pas devant lui un sablier d'une minute pour jouer son coup a_2.

Comme souvent en mathématiques, l'existence d'un objet, bien que prouvée, n'est pas associée à un procédé effectif de construction, ou alors le temps de calcul nécessaire est rédhibitoire.

VII. D'autres jeux diophantiens pour jouer en famille.

Rappelons que B doit annuler pour gagner.

- $J_3 = a_1 - a_2\, b_1\, b_2$

A gagne en choisissant comme stratégie : $a_1 = 1$ puis $a_2 = 0$.
$J_3(a_1, a_2, b_1, b_2) = 1$ ne sera jamais nul quel que soit le choix de B.

- $J_4 = (2b_1 - a_1)(2b_1 - a_1 + 1)$.

B gagne. Le théorème associé est « Tout entier de $\mathbb{N}$ s'écrit $2k$ ou $2k + 1$ ».

- Certains jeux diophantiens sont « ouverts » en ce sens qu'on ne sait pas dire qui est le gagnant !

C'est le cas de $J_5 = (b_1 + a_2)^2 + 1 - (b_2 + 2)(b_3 + 2)$.

A peut rendre $m = b_1 + a_2$ arbitrairement grand, donc B gagnera si et seulement s'il peut factoriser à coup sûr $m^2 + 1$, m étant arbitrairement grand. Mais, à ma connaissance, la démonstration de l'existence d'une infinité de nombres premiers de la forme $m^2 + 1$ n'est toujours pas établie. Si la démonstration est faite un jour, le statut de J_5 deviendra illico « gagnant pour A ».

- Au jeu $Q_1 = (1 + b_1)^3 + (1 + b_2)^3 - b_3^3$, A gagne à cause du théorème de Fermat !

Et depuis la démonstration de Wiles, on sait qu'on peut dans Q_1 remplacer l'exposant 3 par n'importe quel entier supérieur. Remarquez la présence des 1 dans Q_1, sans quoi B gagnerait.

Je propose les deux exercices suivants qu'on peut considérer comme des jeux à moins que ce ne soient des problèmes de maths. Mais y a t-il vraiment une différence ?

- $J_6 = a_1 b_1 b_2 + a_2 - b_3^2 - b_4^2 - b_5^2$.

Il est assez facile de démontrer que A gagne avec par exemple la stratégie $a_1 = 8$; $a_2 = 7$.
Indice : Congruences.

- $J_7 = a_1(1 + b_1) - b_3(2 + a_2^2 - 10b_2)$.

Indice :
Si A joue $a_1 = 0$, B joue $b_3 = 0$ et n'importe quoi pour b_2.
Si A joue $a_1 > 0$, B joue $b_1 = 167$ et selon le résidu modulo 10 du coup a_2 …

VIII. Bibliographie.

Le moins qu'on puisse dire est que la littérature n'est pas bavarde sur le sujet.

GÖDEL, ESCHER, BACH. Les Brins d'une Guirlande Éternelle.
de Douglas HOFSTADTER, *InterÉditions*.

Le dixième problème de Hilbert. Son indécidabilité.
de Youri MATIIASSEVITCH, *Masson*.

250 problèmes de la théorie élémentaire des nombres.
de W. SIERPINSKI, *Hachette*
dans lequel on trouvera sous le label 5/162 l'énoncé et la démonstration du résultat de Lebesque : l'équation $x^2 - y^3 = 7$ n'a pas de solution dans $\mathbb{N}$.

La fabrication d'un jeu diophantien à partir d'un thème imposé, est un exercice passionnant en soi.
Ce serait bien si des lecteurs proposaient des jeux diophantiens qui seraient publiés dans la revue en tant que problèmes mathématiques.