INTRODUCTION

La pensée peut être munie d'objets abstraits qui l'incarnent, la cristallisent, et prennent leur propre vie, se libérant du flux continu et tumultueux des idées. Dans cette naissance du raisonnement, les nombres sont des compagnons rencontrés tôt. Les nombres – entiers tout d'abord – ne sont pas seulement des objets élémentaires du monde mathématique : ils sont également fondamentaux.

La théorie des nombres fournit des problèmes qui, si leur énoncé est remarquablement simple, ont tenu en échec des générations de mathématiciens, pendant plusieurs siècles. C'est que les structures qui vivent dans les nombres sont riches et complexes : en les étudiant sous le prisme de théories mathématiques variées, on y découvre des connexions profondes qui deviennent idées fécondes.

Ce livre n'a aucunement la prétention d'offrir une visite guidée exhaustive de cet univers. On va plutôt s'y balader et choisir sur la carte – au milieu de territoires inconnus – un objectif qui nous permettra d'autant mieux explorer. Au cours de notre voyage, on aura ainsi l'occasion d'étudier la géométrie des nombres, d'observer les symétries de structures algébriques qui s'y cachent, ou de relâcher notre regard pour s'éclipser dans un monde analytique plus lisse.

Notre objectif final, ce point bien localisé sur la carte, a un nom : *l'équation aux S-unités*.

Cadre et objectifs du voyage

Ce voyage mathématique a lieu dans le cadre du Projet Scientifique Collectif (PSC), proposé par l'École polytechnique aux élèves de deuxième année du cycle ingénieur. Nous sommes ainsi 5 à nous y être lancés, guidés et soutenus par notre tuteur, Diego Izquierdo.

L'objectif de cet ouvrage est multiple.

Le premier objectif, qui guide la structure du texte, est la démonstration d'un résultat puissant pour l'étude des équations diophantiennes : la finitude de l'équation aux S-unités. Plus précisément, on s'intéresse à la preuve proposée en 1996 par Beukers et Schlickewei, qu'on placera dans son contexte scientifique et dont on présentera l'intérêt dans la suite de cette introduction.

Notre deuxième objectif a été, en restituant l'ensemble de nos recherches dans un unique texte, de permettre au lecteur d'étudier ce théorème et sa preuve en limitant autant que possible les lectures annexes. En effet, la compréhension de l'article de Beukers et Schlickewei présuppose la connaissance de notions et résultats qui, s'ils sont bien sûr traités dans la littérature, ne sont généralement abordés que dans des cours de niveau M2, voire souvent connus des seuls spécialistes. Notre ambition a donc été de construire un parcours cohérent, permettant au lecteur dès le niveau de L3, voire L2, de comprendre et se construire une intuition du théorème et du monde mathématique qui le soutient. Pour cela, il nous a fallu reconstruire de nombreux résultats intermédiaires, réinterpréter et adapter des démonstrations, etc. : construire une démarche et son intuition.

Notre troisième objectif concerne les utilisations de ce livre : sa quasi-totalité présente des mondes mathématiques qui prennent sens bien au-delà de l'étude de l'équation aux S-unités. Nous avons nous-mêmes tiré énormément partie de nombreux mémoires mis à disposition par leur auteurs, quand bien même ce que nous y cherchions ne représentait qu'une fraction du texte – souvent pas son objectif final. Nous espérons ainsi que cet ouvrage saura trouver des lecteurs pour lesquels il sera un apport dans leurs propres recherches.

Contexte scientifique : le monde diophantien

La question scientifique centrale, qui fait naître les théories développées dans ce livre, est la suivante : comment étudier les équations – polynomiales – à solutions entières ? On parle d'*équations diophantiennes*.

S'il peut sembler plus naturel de chercher les solutions de ces équations dans les entiers, qui sont a priori des objets plus simples que les réels par exemple, cette restriction rend en fait le problème beaucoup plus difficile – on pourra aussi dire que c'est ce qui en fait le charme.

Au-delà du charme, pourquoi chercher des solutions entières ? C'est le naturel qui revient : en logistique, et donc en optimisation opérationnelle, on travaille souvent *in fine* avec une quantité entière d'objets. De ce fait, ces problèmes sont généralement très difficiles ! En informatique, l'univers est fini et discret : il faut le comprendre pour aborder la cryptographie, la compression et la correction automatique de signaux, ou quantité d'autres domaines. Plus généralement, on peut se contenter de dire que les nombres entiers sont fondamentaux et réapparaissent naturellement lors de l'étude de nombreux objets.

On peut aborder un point de vue géométrique sur cette question : étudier les solutions entières d'équations polynomiales, c'est *étudier les points entiers de variétés algébriques*.

Les question sont alors les suivantes. Est-ce qu'il y a des points entiers ? Est-ce qu'il y en a beaucoup ? À quelle densité ? Un nombre fini ? Y a-t-il une structure sur ces points, algébrique ou géométrique ?

C'est la morale moderne du monde diophantien, nourri de géométrie algébrique : les propriétés arithmétiques sont contrôlées par des propriétés géométriques !

Historiquement,

- Pendant plusieurs siècles, seules quelques équations particulières ont pu être traitées, laborieusement, souvent de façon ad-hoc et au cas par cas.
- Une prise de recul permet néanmoins de construire de puissants outils et stratégies au XVII^e et XVIII^e siècle.

  Au XVIIème Fermat introduit quelques grands problèmes (l'équation de Pell-Fermat sur laquelle on reviendra plusieurs fois, ou la dernière conjecture de Fermat qui n'est devenue le théorème de Fermat-Wiles que trois siècles plus tard en 1994), et propose des démonstrations par descente infinie – certaines erronées – de divers résultats sur des équations particulières.

  Le siècle suivant, Euler, Lagrange, Legendre et Gauss font partie de ceux qui développent la profondeur théorique du domaine. Par exemple, de premiers travaux en théorie analytique des nombres sont entrepris, et la loi de réciprocité quadratique est démontrée.
- Le XIX^e siècle amène un enrichissement conséquent de la théorie des nombres. Pour ne retenir qu'un nom, évoquons celui de Dirichlet : on le retrouvera de nombreuses fois dans ce livre, par exemple aux chapitre 3 où on parlera de l'arithmétique des idéaux, qui permet de généraliser la notion de décomposition en facteurs premiers à des anneaux qui n'en admettent pas, ou quand on montrera au chapitre 4 le *théorème des unités de Dirichlet*, profond résultat de théorie algébrique des nombres.
- Grâce à cette nouvelle profondeur, le début du XX^e siècle conçoit enfin les premiers outils généraux pour aborder les équations diophantiennes. On voit ainsi apparaître la théorie des hauteurs (introduite aux chapitres 5 et 6), qui mesure la complexité algébrique de solutions d'équations diophantiennes, ou des méthodes dues à Axel Thue qui s'appuient sur l'approximation diophantienne mais qu'on n'aborde pas ici.

  C'est en 1909 que Thue démontre un théorème qui sera peu à peu amélioré pour aboutir en 1996 au résultat de Beukers et Schlickewei qu'on étudie ici.

On en reparlera un peu plus tard, mais on peut déjà dire ceci : il s'agit, enfin, d'un résultat de finitude non trivial qui peut s'appliquer à une large classe d'équations.

- En 1983 Gerd Faltings démontre un résultat majeur, très profond, qui lui vaudra la médaille Fields en 1986. Quand on dit que « les propriétés arithmétiques sont contrôlées par des propriétés géométriques », ont fait largement référence à ça. On cite ce théorème de façon informelle. Il est la démonstration d'une conjecture émise par Louis Mordell en 1922, qui avait par ailleurs démontré en 1920 un théorème qu'on va citer par la même occasion.

  Théorème 1 (Théorème de Faltings)**.** *Considérons une courbe algébrique C définie, pour un polynôme $P \in \mathbb{Q}[X, Y]$, par l'équation*

  $$(C) \ : \ \ P(x, y) = 0.$$

  On cherche à caractériser le nombre X de points de C à coordonnées rationnelles.
  ***Le nombre de solutions dépend du genre de** C (qui correspond intuitivement à son nombre de trous).*

  - *Si le genre vaut 0, alors $X = 0$ ou $X = \infty$.*
  - *Si le genre vaut 1, alors $X = 0$ ou C est une courbe elliptique. Dans ce deuxième cas, Mordell a montré en 1920 que l'on pouvait munir les points rationnels de C d'une structure de groupe abélien de type fini.*
  - *Si le genre est plus grand ou égal à 2, alors $X < \infty$. C'est le point démontré par Faltings.*

- Le théorème de Faltings est très puissant, mais il n'est absolument pas explicite. En particulier, dans le cas de finitude, on n'a aucune borne sur la densité de solutions, voire sur le nombre de solutions. Un domaine de recherche actuel très actif consiste à *expliciter Faltings*, de façon à pouvoir par exemple s'en servir dans des algorithmes ou dans des raisonnements numériques. C'est là qu'intervient l'équation aux S-unités : elle fournit un angle d'attaque intéressant, puisque le théorème de finitude associé est au contraire très explicite.

Avant d'enfin énoncer le théorème de l'équation aux S-unités, présentons rapidement quelques classes d'équations diophantiennes particulières qu'il est intéressant d'étudier.

- On en reparlera plus tard, mais les grandes équations historiques ont bien sûr un intérêt illustratif. Citons l'équation de Pell-Fermat, sur laquelle on reviendra. Il

s'agit de considérer $n \in \mathbb{N}$ qui n'est pas un carré parfait, $m \in \mathbb{Z}^*$, et d'étudier les solutions $x, y \in \mathbb{Z}$ de

$$x^2 - ny^2 = m.$$

- Le théorème de Mordell (énoncé plus haut) s'applique aux courbes elliptiques, et participe à leur conférer un intérêt particulier.

  Elles apparaissent à la fois dans un nombre croissant d'applications informatiques et dans des questions profondes de mathématiques pures. Elles apparaissent par exemple dans la conjecture de Shimura-Taniyama-Weil, en lien avec des « courbes modulaires » : la démonstration de cette conjecture a permis de démontrer le théorème de Fermat-Wiles. On peut également citer la conjecture de Birch et Swinnerton-Dyer, un des sept problèmes du millénaire (à ce jour seule la conjecture de Poincaré a été résolue par Grigori Perelman), qui s'énonce en reliant avec elles des objets analytiques.

  Informellement, elles sont décrites par les équations de la forme suivante, où $f \in \mathbb{Q}[X]$ est un polynôme unitaire de degré 3 :

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

- Nous venons de le dire, le théorème de Mordell s'applique aux courbes elliptiques : elles sont de genre 1. Pour voir plus large que cette contrainte, on peut s'intéresser aux courbes *hyperelliptiques*, définies par les équations de la forme suivante, où $f \in \mathbb{Q}[X]$:

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

  Le genre de la courbe est alors contrôlé par le degré de f.

Le théorème

Le décor étant placé, passons enfin à l'énoncé du théorème dont la démonstration est l'objectif final de ce livre.

On parlera de son histoire dans la partie suivante, puis on présentera quelques applications (qui ne seront pas étudiées dans ce texte).

On va maintenant présenter l'équation aux S-unités dans le contexte de $\mathbb{Z}$, puis dans un contexte plus général, puis montrer sur un cas élémentaire non trivial que ses solutions sont en nombre fini. Remarquez la simplicité de cette équation : c'est ce qui explique que de nombreux problèmes diophantiens s'y ramènent.

• Un premier cadre pour l'équation : $\mathbb{Z}_S$

Dans $\mathbb{Z}$, l'équation aux S-unités peut s'énoncer de la manière suivante.
Étant donné S un ensemble fini de nombres premiers, on se demande si l'équation

$$x + y = z$$

admet un nombre fini de solutions $(x, y, z) \in \mathbb{Z}^3$ telle que x, y, z sont deux à deux premiers entre eux et ont tous leurs facteurs premiers dans S.

On peut d'ores et déjà réécrire cette équation en posant $S = \{p_1, ..., p_s\}$ et $\mathbb{Z}_S$ l'anneau $\mathbb{Z}[p_1^{-1}, ..., p_s^{-1}]$. L'équation aux S-unités devient alors

$$x + y = 1,$$

où $x, y \in \mathbb{Z}_S^\times$, l'ensemble des éléments inversibles de $\mathbb{Z}_S$, qui peut-être ici explicité :

$$\mathbb{Z}_S^\times = \Big\{ \pm\, p_1^{r_1} ... p_s^{r_s} \,\Big|\, p_i \in S,\, r_i \in \mathbb{Z} \Big\}.$$

Avec cette formulation, on dispose du théorème suivant, démontré par le mathématicien d'origine allemande Kurt Mahler en 1933 [1].

Théorème 2 (Mahler, 1933)**.** *Soit $S = \{p_1, ..., p_s\}$ un ensemble de nombres premiers distincts. L'équation d'inconnues $x, y \in \mathbb{Z}_S^\times$*

$$x + y = 1$$

admet un nombre fini de solutions.

Mahler propose déjà en 1933 une borne du nombre de solutions, mais elle est très mauvaise et apporte peu d'informations.

Il est possible de considérer ce résultat sur des structures plus générales.

• Le cadre général de $\mathcal{O}_{K,S}$

Dans la première expression de l'équation, on travaillait dans $\mathbb{Z}_S$ qui était un sous-anneau de $\mathbb{Q}$. L'idée est maintenant de voir ce qui se passe pour des corps plus gros, mais qui ont toujours des propriétés assez agréables pour qu'on puisse y formuler le problème.

On verra dans ce livre que ce cadre naturel est celui des corps de nombres, c'est-à-dire des extensions finies de $\mathbb{Q}$.

Dans le cas de K un corps de nombres, on verra que c'est l'anneau des entiers algébriques de K, noté $\mathcal{O}_K$, qui joue un rôle analogue à $\mathbb{Z}$ en préservant certaines propriétés, par exemple une certaine notion de primalité. La reformulation est alors la suivante.

Définition 0.0.1. Soient K un corps de nombres et $S = \{a_1, ..., a_s\} \subset \mathcal{O}_K$ un ensemble fini. On définit $\mathcal{O}_{K,S}$ par

$$\mathcal{O}_{K,S} = \mathcal{O}_K[a_1^{-1}, ..., a_s^{-1}].$$

Ainsi, si on note $\langle S \rangle$ la partie multiplicative engendrée par S, c'est à dire l'ensemble des produits d'éléments de S, on a

$$\mathcal{O}_{K,S}^{\times} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \langle S \rangle \right\}.$$

$\mathcal{O}_{K,S}^{\times}$ est donc en quelque sorte « K^* restreint à $\langle S \rangle$ ».

De façon analogue au cas entier, on a le résultat suivant, démontré en 1996 par Beukers et Schlickewei [2].

Théorème 3 (Beukers et Schlickewei, 1996)**.** *Soit K un corps de nombres. Soit $S \subset \mathcal{O}_K$ un ensemble fini. L'équation d'inconnues $(x, y) \in (\mathcal{O}_{K,S}^{\times})^2$*

$$x + y = 1$$

admet un nombre fini de solutions.

De plus, ce nombre de solutions est borné par 2^{16r+8}, où r est le rang sans torsion de $\mathcal{O}_{K,S}^{\times}$ en tant que groupe abélien de type fini, et est donné par le théorème des S-unités de Dirichlet (théorème 12 de ce texte).

En fait, comme on le verra au dernier chapitre, le résultat montré par Beukers et Schlickewei est plus général et ne s'applique pas qu'à $\mathcal{O}_{K,S}^{\times}$, bien que cet exemple en soit la motivation.

• Un cas élémentaire

Avant d'aller plus loin, regardons ce qu'il se passe dans le cas non trivial le plus simple. Plaçons-nous dans le cadre de la première formulation : $K = \mathbb{Q}$ et $\mathcal{O}_K = \mathbb{Z}$. Prenons $S = \{2, 3\}$. On a donc l'expression

$$\mathbb{Z}_S^{\times} = \{\pm 2^r 3^s \mid r, s \in \mathbb{Z}\}.$$

Autrement dit, résoudre l'équation

$$x + y = 1 \quad \text{où } x, y \in \mathbb{Z}_S^{\times}$$

revient à trouver deux couples (r_1, s_1) et (r_2, s_2) de $\mathbb{Z}^2$ tels que

$$\pm 2^{r_1} 3^{s_1} \pm 2^{r_2} 3^{s_2} = 1.$$

On voit d'abord que cela revient à résoudre l'équation

$$2^r - 3^s = \pm 1 \quad \text{où } r, s \in \mathbb{N}. \tag{1}$$

En effet, si on a une solution avec des exposants strictement négatifs, on peut nettoyer les expressions et évaluer modulo 2 ou 3 soit pour conclure à une absurdité, soit pour se ramener au cas entier. Enfin, si on a uniquement des puissances positives, une évaluation modulo 2 ou 3 permet encore de conclure qu'on est dans le cas de l'équation (1). On épargne au lecteur ces détails. Passons à la résolution de l'équation.

On distingue le cas 1 ou -1.

Premier cas

$$2^r - 3^s = 1 \quad \text{où } r, s \in \mathbb{N}.$$

- Si $r = 0$, il n'y a pas de solution.
- Si $r = 1$, l'unique solution est $s = 0$.
- Si $r = 2$, l'unique solution est $s = 1$.
- Si $r \geq 3$, on remarque que $2^r \equiv 0[8]$. En raisonnant sur la parité de s on remarque que $3^{2k} \equiv 1[8]$ et $3^{2k+1} \equiv 3[8]$. Aucun couple (r, s) ne nous permet donc d'avoir $2^r - 3^s = 1$.

Second cas

$$2^r - 3^s = -1 \quad \text{où } r, s \in \mathbb{N}.$$

- Si $r = 0$, pas de solution.
- Si $r = 1$, l'unique solution est $s = 1$.
- Si $r = 2$, pas de solution.
- Si $r \geq 3$, on distingue à nouveau selon les valeurs de s.
  - Si s est impair, alors $3^s \equiv 3[4]$ et $2^r - 3^s \equiv -3 = 1[4]$: pas de solution.
  - Si $s = 4k$ alors $3^s - 1 \equiv 0[5]$ et $3^s - 1$ n'est pas une puissance de 2 : pas de solution.
  - Si $s = 4k + 2$ alors $3^s - 1 \equiv 8[16]$ et on ne peut pas avoir $3^s - 1 = 2^r$ puisque $r \geq 3$.

Ainsi on a bien un nombre fini de solutions, et le théorème de Malher est vérifié. On voit bien à travers cet exemple que des stratégies « ad-hoc » vont parfois permettre de résoudre les cas particuliers, mais sûrement pas d'obtenir un résultat général.

Cela représente bien la situation des équations diophantienne, et explique pourquoi les résultats au sujet de ces équations ont été aussi tardifs (majoritairement au XIX^e et XX^e siècle), alors qu'elles sont étudiées depuis l'Antiquité.