

III. ETUDES

Diophante et la tradition diophantienne

L'époque de la vie de DIOPHANTE D'ALEXANDRIE est fort incertaine. Il fleurissait peut-être dans la seconde moitié du III^e siècle. Ses *Arithmétiques* sont un recueil assez confus de problèmes numériques, compilés, au moins en partie, sur des sources antérieures remontant au moins jusqu'à l'école de Pythagore, si ce n'est jusqu'à la Mathématique babylonienne. De ces problèmes, les uns sont déterminés, mais la plupart sont indéterminés, avec la condition que les solutions soient rationnelles. DIOPHANTE se contente d'ailleurs d'une solution particulière, obtenue au moyen d'artifices qui ne se prêtent pas à la généralisation. Le système des notations se réduit à des abréviations et ne comporte que la représentation d'une seule inconnue, dont les diverses puissances, jusqu'à la sixième, et leurs inverses, ont des symboles spéciaux.

Il y a là une ébauche de notation, encore fort insuffisante, en particulier du fait qu'une seule inconnue peut être utilisée. Mais cette insuffisance même du symbolisme oblige le mathématicien à une grande habileté dont en fin de compte la science a profité.

Pour donner un aperçu des procédés de DIOPHANTE, prenons dans la traduction VER ECKE quelques exemples précis :

Livre II, proposition XX : « Trouver deux nombres tels que le carré de chacun d'eux, diminué du nombre restant, forme un carré.

« Que le plus petit nombre soit 1 arithme accru d'autant d'unités qu'on voudra, notamment de 1 unité, et que le plus grand nombre soit le carré du plus petit nombre, à moins d'un carré d'arithme, afin que le carré du plus petit nombre, diminué du plus grand nombre, forme un carré » (le petit nombre est $x + 1$, le grand $(x + 1)^2 - x^2$, la différence entre le carré du petit et le grand est alors x^2).

« Dès lors, puisque le carré du plus petit nombre est 1 carré d'arithme plus 2 arithmes plus 1 unité, il s'ensuit que le plus grand nombre sera ce qui est ajouté au carré de l'arithme, c'est-à-dire 2 arithmes plus l'unité $[(x + 1)^2 - x^2 = 2x + 1]$, et il s'établit ainsi que le carré du plus petit nombre, diminué du plus grand, forme un carré. Il faut aussi que le carré du plus grand nombre, c'est-à-dire 4 carrés d'arithme, plus 4 arithmes plus 1 unité, diminué du plus petit nombre, forme un carré. Mais le carré du plus grand nombre, diminué du plus petit nombre, donne 4 carrés d'arithme plus 3 arithmes, ce que nous égalerons à un carré. Formons le carré de 3 arithmes, et l'arithme devient $3/5$ ($4x^2 + 3x = 9x^2$, $x = 3/5$). Le plus petit nombre sera $8/5$; le plus grand nombre sera $11/5$, et ces nombres satisfont à la proposition. »

Livre IV, proposition XXIV : « Partager un nombre donné en deux nombres, et faire en sorte que le produit de ces nombres soit un cube à moins de la racine de ce cube.

« Que le nombre donné soit 6. Posons que le premier nombre est 1 arithme, et il s'ensuit que le second nombre restant sera 6 unités moins 1 arithme. (Il faut donc résoudre $x(6 - x) = y^3 - y$).

« Il faut encore avoir que le produit de ces nombres soit un cube à moins de sa racine. Mais le produit des nombres sera 6 arithmes moins 1 carré d'arithme, ce qui doit être égal à un cube à moins de sa racine. Formons le cube d'une quantité quelconque d'arithmes moins 1 unité, notamment, le cube de 2 arithmes moins 1 unité. Le cube de cette expression, diminué de cette expression même, forme 8 cubes d'arithmes plus 4 arithmes moins 12 carrés d'arithme ; ce que nous égalons à 6 arithmes moins 1 carré d'arithme. (On pose $y = 2x - 1$, d'où $y^3 - y = 8x^3 + 4x - 12x^2$, et l'équation $6x - x^2 = 8x^3 + 4x - 12x^2$).

« Or, si les quantités d'arithmes étaient égales de part et d'autre dans l'équation, il resterait des cubes d'arithmes égaux à des carrés d'arithmes et l'arithme serait rationnel. (Si les coefficients de x étaient égaux dans les deux membres, l'équation aurait une racine rationnelle évidente ; il s'agit désormais de modifier les hypothèses arbitraires du début de la solution pour arriver à ce cas particulier, et nous saisissons ici sur le vif un raisonnement purement analytique). Mais 4 arithmes proviennent d'un excédent sur 2 arithmes, notamment de l'excédent de trois fois 2 arithmes. D'autre part, si trois fois 2 arithmes sont diminués de 2 arithmes, ils forment deux fois 2 arithmes, tandis que 6 a été pris arbitrairement par hypothèse. Dès lors, nous sommes amenés à trouver, comme pour 2, qui est la quantité d'arithmes, un nombre qui, pris deux fois, forme 6. Or, ce nombre est 3. En conséquence, cherchons à égaler 6 arithmes moins 1 carré d'arithme à un cube à moins de sa racine. Posons maintenant que la racine du cube est 3 arithmes moins 1 unité ; le cube de cette racine, diminué de cette racine même, forme 27 cubes d'arithme plus 6 arithmes moins 27 carrés d'arithme, ce que nous égalons à 6 arithmes moins 1 carré d'arithme, et l'arithme devient 26/27.

« Revenant aux choses posées, le premier nombre sera 26/27, et le second sera 136/27. »

Le livre VI, le dernier des treize livres qui soit arrivé jusqu'à nous, s'occupe des triangles rectangles en nombres. On savait depuis les anciens Babyloniens trouver un triangle rectangle dont les côtés soient mesurés par des entiers. Si m et n sont deux nombres premiers entre eux de parités différentes, et l un entier quelconque, les trois côtés du triangle sont : $l(m^2 + n^2)$, $l(m^2 - n^2)$ et $2lmn$.

Voici quelques énoncés de problèmes du livre VI :

I. — « Trouver un triangle rectangle tel que le nombre de l'hypoténuse, diminué de chacun des nombres des perpendiculaires, forme un cube. »

La solution consiste à poser $l = 1$, $m = x$, $n = 3$, d'où l'équation : $x^2 + 9 - x^2 + 9 =$ un cube, mais 18 ou $2n^2$ n'est pas un cube, prenons donc $n = 2$, et une des conditions du problème est satisfaite. Il faut de plus que $m^2 + n^2 - 2mn$ soit un cube, ou $x^2 + 4 - 4x$, carré de $x - 2$. Egalons donc $x - 2$ à un cube, 8 par exemple. Il vient $x = 10$, et le triangle a pour côtés 104, 96 et 40.

III. — « Trouver un triangle, rectangle, tel que le nombre de son aire, augmenté d'un nombre donné, forme un carré. »

Réponse : $l = 1$, $m = 24/5$, $n = 5/24$, le nombre donné étant 5.

IX. — « Trouver un triangle rectangle, tel que le nombre de son aire, diminué du nombre constituant la somme de ses perpendiculaires, forme un nombre donné. »

Le nombre donné étant 6, le triangle aura pour côtés : $\frac{18}{35}$, $\frac{270}{35}$
 et $\frac{168}{35}$.

XXI. — « Trouver un triangle rectangle, tel que le nombre de son périmètre soit un carré, et que ce périmètre, augmenté du nombre de l'aire du triangle, forme un cube. »

Ces quelques exemples suffiront à dégager les caractéristiques de l'Algèbre de DIOPHANTE. Il y a là une Mathématique toute gratuite, sans applications pratiques immédiates, une sorte d'art pour l'art, qui ne pouvait s'épanouir que dans des écoles et être cultivée par des professionnels de l'enseignement. En cela, elle se distingue nettement du courant plus pratique qui apparaît dans ARCHIMÈDE, HÉRON ou PTOLÉMÉE. Il n'empêche qu'il y a là un aspect très vivace de la science mathématique, qui remonte d'une part aux exercices des Babyloniens et qui, d'autre part, fera sentir son influence, très nette et très salutaire, aux XVI^e et XVII^e siècles.

L'ancienne analyse diophantienne

L'analyse des nombres rationnels, ou analyse diophantienne, se propose, comme nous l'avons vu au sujet de DIOPHANTE, de résoudre des systèmes d'équations indéterminées où les données et les inconnues sont des nombres rationnels.

Abordée sporadiquement, sous des influences arabes, par les mathématiciens du XII^e siècle, LÉONARDO PISANO particulièrement, elle ne prend un essor notable qu'au XVI^e siècle, lorsque l'œuvre diophantienne commence à être connue directement par l'Occident. BOMBELLI en traite longuement, dans une sorte de paraphrase des Arithmétiques de DIOPHANTE, dans son Algèbre de 1572. Ce travail y fait l'objet du livre III où sont étudiés 143 problèmes dont 35 sont tirés du premier livre de DIOPHANTE, 27 du second, 21 du troisième, 40 du quatrième et 20 du cinquième. Les deux premiers livres de l'Algèbre de BOMBELLI résument l'évolution purement italienne de la science, en particulier la résolution des équations des quatre premiers degrés, et l'introduction des imaginaires.

Au moment de la parution du travail de BOMBELLI, l'Allemand Guillaume HOLZMANN, ou XYLANDER, s'occupait de la traduction latine des Arithmétiques de DIOPHANTE, traduction qu'il publia à Bâle en 1575. Dès 1577, GOSSELIN de Caen, dans son Algèbre latine publiée à Paris, s'inspirait des méthodes diophantiennes dans le troisième livre, chapitres 11 et 12, où il traitait particulièrement de la double équation.

C'est ici le lieu d'indiquer ce qu'était le problème de la double équation. Il s'agissait essentiellement de trouver des valeurs des deux inconnues x et y qui rendent à la fois carrés parfaits deux polynômes donnés en x et en y . Par exemple (DIOPHANTE, Liv. 2, prop. 20) : « Trouver deux

nombres tels que le carré de chacun d'eux, accru du nombre restant, forme un carré », ou (Liv. 2, prop. 11) : « Ajouter un même nombre à deux nombres donnés, de manière que chacun d'eux forme un carré. »

Ni DIOPHANTE, ni ses imitateurs du xvi^e siècle ne cherchent une solution générale. Ils se contentent tous d'une solution particulière. Par ailleurs, bien entendu, les données sont purement numériques, et une seule inconnue est utilisée.

Si XYLANDER s'efforce de donner une traduction fidèle du texte de DIOPHANTE, BOMBELLI et GOSSELIN, plus libres par les buts qu'ils s'assignent, ne craignent pas d'utiliser leurs propres notations algébriques dans la résolution des problèmes indéterminés.

Simon STÉVIN, ce savant universel, dont on a trop tendance, en France, à sous-estimer l'influence, dans son ouvrage de 1585, écrit en français, sous le titre « L'Arithmétique de Simon STÉVIN de Bruges... », annonce « les quatre premiers livres d'Algèbre de DIOPHANTE, d'Alexandrie, maintenant premièrement traduits en français ». En fait, on ne trouve dans cet ouvrage que de simples adaptations de 81 propositions des quatre premiers livres de DIOPHANTE, dans les notations algébriques de STÉVIN, voisines de celles de BOMBELLI.

Enfin, François VIÈTE publie à Tours, en 1593, ses cinq livres de problèmes, ou Zététiques, *Zeteticorum libri V*, ouvrage d'Analyse Diophantienne, traduit en français et publié par VAU LÉZARD en 1630 sous le titre « *Les cinq livres des Zététiques de François VIÈTE* ». A l'encontre des auteurs précédents, le grand analyste ne se contente pas d'appliquer les méthodes de DIOPHANTE, mais il les étend et les utilise pour la résolution des problèmes les plus difficiles. VIÈTE ne craint d'ailleurs pas, dans cet ouvrage, d'utiliser parfois les méthodes du savant grec à des problèmes où la variable est continue, et qui sortent par suite de l'analyse indéterminée. On peut dire à cet égard que se dessine chez lui une évolution qui fera passer d'une étude des nombres rationnels à une étude des fonctions rationnelles, étude qui sera des plus utiles pour les créateurs du calcul intégral. Le problème : rendre rationnelle par un changement de variable, lui-même rationnel, l'expression :

$$\sqrt{ax^2 + bx + c}$$

relève en effet des méthodes mêmes de DIOPHANTE, et son importance dans les intégrations est considérable. On le résoudra, soit en posant

$$ax^2 + bx + c = (xt + \sqrt{c})^2, \text{ si } c > 0,$$

soit en posant $ax^2 + bx + c = (x\sqrt{a} + t)^2$, si $a > 0$. Un changement linéaire de variable pouvant toujours ramener l'expression, lorsqu'elle est réelle, à un de ces cas, le problème de l'intégration d'une fonction irrationnelle se ramène pour un homme comme Jean BERNOULLI à un problème diophantien.

En 1621, BACHET de Méziriac publie à Paris sa célèbre édition grecque du Diophante, précédée de porismes et accompagnée d'une traduction et d'un abondant commentaire latin.

L'influence sur FERMAT de cette édition de DIOPHANTE fut considérable. Son fils en publia en 1670, à Toulouse, une réédition enrichie des

remarques de son père, remarques où sont consignées plusieurs de ses découvertes en théorie des nombres, et dont nous parlerons plus loin. En Analyse diophantienne proprement dite, les découvertes de FERMAT sont exposées principalement dans un ouvrage annexe à l'édition de son fils, *Doctrinæ Analyticæ Inventum Novum*, du Père Jacques DE BILLY. Ce travail est extrait des lettres que FERMAT adressa à son auteur qui déclare (1) : « ...Je veux dès maintenant dire en quelques mots quelles récentes découvertes lui sont dues et quelle en est la portée. En premier lieu, il y a certaines équations doubles difficiles pour lesquelles les analystes n'ont pu jusqu'à présent trouver qu'une solution unique ; BACHET lui-même affirme qu'on ne peut en trouver deux, tandis que FERMAT va en donner tout à l'heure une infinité, sans être arrêté par les nombres faux et plus petits que zéro qui se présentent souvent dans les calculs de ce genre ; il les soumettra en effet à un subtil traitement qui les réduit immédiatement à des nombres vrais. En second lieu, personne, que je sache, n'a encore résolu l'équation triple, à moins de l'avoir d'avance formée artificiellement et combinée de telle sorte que la solution en apparaisse immédiatement, même aux yeux des novices ; FERMAT a trouvé une méthode singulière pour résoudre les équations arbitrairement proposées de ce genre, en exceptant un seul cas que nous indiquerons ci-après. En troisième lieu, qui jamais a donné autant de solutions que l'on veut pour les expressions composées de cinq termes de degrés successifs ? Qui, des racines primitives, a su en tirer de dérivées du premier ordre, du second, du troisième, et ainsi de suite indéfiniment ? Personne, sans doute ; à FERMAT seul appartient cette découverte. Il n'a pas puisé ces inventions dans les ouvrages d'autrui, comme ont coutume de le faire certains arrangeurs, il les a tirées de son propre fonds, élaborées lui seul... »

Prenons maintenant quelques exemples dans l'*Inventum Novum*. Soit la double équation $-2x + 1 = \square$ $2x^2 - 4x + 1 = \square$. Il s'agit d'égaliser à des carrés les deux premiers membres. La méthode classique alors connue consistait à mettre leur différence $2x^2 - 2x$ sous forme d'un produit $2x(x - 1)$, et d'égaliser la seconde des deux expressions au carré de la demi-somme des deux facteurs $(2x - 1)^2$. On trouve la solution sans intérêt $x = 0$. En prenant les facteurs x et $2x - 2$, de demi-somme $\frac{3}{2}x - 1$, on a $2x^2 - 4x + 1 = \frac{9}{4}x^2 - 3x + 1$, d'où $x = -4$. « Cette solution, écrit DE BILLY, est, je l'avoue, un faux nombre, cependant elle peut servir à trouver des nombres vrais. Prenez $x = -4$ comme nouvelle position de l'inconnue, et substituez dans les expressions proposées ; elles deviendront $-2x + 9$ et $2x^2 - 20x + 49$,... Dans les expressions transformées, les termes indépendants de x sont carrés ; la méthode de DIOPHANTE permet donc de trouver une valeur de x . » (On égalera à des carrés, non les expressions données, mais leurs produits respectifs par 49 et par 9, et on procédera comme plus haut). « J'en retrancherai 4, puis-

(1) Traduction de P. Tannery, *Œuvres*, de FERMAT, C. III, p. 326.

que j'ai pris $x = 4$ pour représenter l'inconnue ; j'aurai ainsi une solution $\frac{5333240}{39150049}$ pour le système proposé. Ainsi, le faux nombre a permis d'en trouver un vrai qui satisfait au problème, comme on peut le vérifier. »

« C'est un champ très fertile que celui que nous avons commencé à cultiver ; car la méthode de FERMAT peut fournir une infinité de solutions non seulement pour les doubles équations, mais encore pour les autres. Soit à évaluer à un cube $8x^2 - 12x + 8$.

Prenons $2 - x$ pour racine de ce cube ; on aura $8 - 12x + 6x^2 - x^3 = 8x^2 - 12x + 8$, d'où $x = -2$, faux nombre qui satisfait à la question. Pour en avoir un vrai, substituons $x - 2$ à x dans l'expression proposée $8x^2 - 12x + 8$; la transformée sera $8x^2 - 44x + 64$ à évaluer à un cube.

On prendra pour racine de ce cube $4 - \frac{11}{12}x$ (4 étant la racine cubique de 64..., $\frac{11}{12}x$ est le quotient obtenu en divisant $44x...$ par 3 fois le carré de la racine cubique 4...), d'où je tire $x = 2 \frac{938}{1331}$. Si je retranche 2, puis-que j'ai pris $x - 2$ pour représenter l'inconnue, j'aurai pour celle-ci la valeur $\frac{938}{1331}$. »

Ces citations donneront une idée de la méthode de FERMAT, à certains égards moins en avance que celle de VIÈTE, à d'autres très supérieure, par exemple lorsque le nombre négatif est utilisé. Une étude plus complète deviendrait rapidement trop technique pour que nous insistions.

Après FERMAT, l'analyse diophantienne continue à être très cultivée, sans que toutefois aucun grand nom de mathématicien ne soit à signaler dans ce domaine au cours du XVII^e siècle. Sous l'influence de VIÈTE, la méthode évolue cependant vers une étude des fonctions rationnelles, comme nous l'avons signalé. Les notations employées sont celles de DESCARTES. En France, citons en plus du Père DE BILLY, OZANAM, dont un manuscrit, *Les six livres de l'Arithmétique de Diophante, augmentés et réduits à la spécieuse*, qui a d'ailleurs disparu, indique bien par son titre l'influence de VIÈTE.

Voici un exemple de sa méthode, tiré de son dictionnaire mathématique, édition de 1691 : « Trouver trois nombres quarréz, tels que la somme de deux quelconques soit un nombre quarré.

« Formez de ax et de by ce triangle rectangle $2abxy$, $aaxx - bbyy$, $aaxx + bbyy$; et réciproquement de bx et de ay . Ce triangle rectangle $2abxy$, $aayy - bbxx$, $aayy + bbxx$, et mettez la hauteur commune $2abxy$, et les deux bases $aaxx - bbyy$, $aayy - bbxx$, pour les côtes des trois quarréz qu'on cherche, lesquels par conséquent seront tels $4aabbxxyy$, $a^4x^4 - 2aabbxxyy + b^4y^4$, $a^4y^4 - 2aabbxxyy + b^4x^4$, car ainsi le premier fera avec chacun des deux autres un nombre quarré, par la nature du triangle rectangle, et il ne reste plus qu'à évaluer au quarré la somme des deux derniers $a^4x^4 + b^4x^4 - 4aabbxxyy + a^4y^4 + b^4y^4$. Pour cette fin, supposez $x = z - \frac{ay}{b}$, et vous aurez en entiers cette autre puissance à

égaler au quarré, $a^8y^4 - 2a^4b^4y^4 + b^8y^4 + 4a^3b^5zy^3 - 4ba^7zy^3 + 6a^6bbyyzz + 2aab^6yyzz - 4a^5b^3zy^3y - 4ab^7z^3y + a^4b^4z^4 + b^8z^4$, pour le côté duquel prenant $a^4yy - b^4yy - 2a^3bzy + \frac{a^6bbzz + aab^6zz}{a^4 - b^4}$ on trouvera $y = b^9 - 2a^4b^5 - 3a^8b$ et $z = 4ab^8 - 4a^9$, et conséquemment $x = 3ab^8 + 2a^5b^4 - a^9$, et les côtes des trois quarréz qu'on cherche seront tels :

$$\begin{aligned} 6aab^{18} - 8a^6b^{14} - 28a^{10}b^{10} - 8a^{14}b^6 + 6bba^{18}, \\ a^{20} - 13a^{16}b^4 - 14a^{12}b^8 + 14a^8b^{12} + 13a^4b^{16} - b^{20}, \\ 8a^{18}bb + 16a^{14}b^6 - 16a^6b^{14} - 8aab^{18}. \end{aligned}$$

« Si l'on suppose $a = 1$ et $b = 2$, les trois quarréz qu'on cherche seront tels, 1995529167424, 20464733025, 5561295897600, dont les côtes sont 1412632, 143055, 2358240. »

Le Père PRESTET consacre presque tout le second volume de ses *Nouveaux Eléments des Mathématiques*, Paris, 1689, à l'Analyse indéterminée. « J'ai résolu, écrit-il dans sa préface, toutes les questions de DIOPHANTE à cause de l'estime qu'on en fait généralement, et du soin que des auteurs illustres ont pris de les commenter. Si l'on compare leur méthode avec celle-ci, on verra l'extrême différence qui s'y trouve. J'ai résolu d'une manière générale toutes les questions qui sont déterminées, et d'une manière infinie et le plus souvent sans restriction celles qui sont indéterminées. Et, lorsque j'ai mis des restrictions, j'en ai mis le moins que j'ai pu, afin de conserver une plus grande étendue dans les résolutions infinies que je découvrirais. J'ai ajouté partout les formules littérales des résolutions générales et des résolutions infinies, afin que l'on eût dans ce volume comme une table déjà résolue des questions de DIOPHANTE, et de beaucoup d'autres qui sont d'un grand usage, comme celles des doubles et des triples égalitez... »

Voici un exemple qui montre combien ces problèmes intéressaient les mathématiciens français à l'époque même de l'invention du nouveau calcul infinitésimal. On lit page 233 de son traité :

« J'ajouterai seulement ici, pour faire encore mieux voir en particulier l'usage et l'application des triples égalités, la résolution d'un problème qui a été proposé à Messieurs de l'Académie Royale des Sciences, et sur lequel ils ont bien voulu travailler. M. OZANAM en a déjà fourni trois ou quatre résolutions différentes dans un traité des lignes qui commence à paraître, et on pourrait en fournir beaucoup d'autres. Celle que je donne ici sera tirée d'une triple égalité, où l'on arrive d'abord avec une extrême facilité et sans rien supposer. J'en tirerai ensuite quelques résolutions, qui s'y rapportent naturellement. Le problème peut être posé en ces termes :

« Pour couper une grandeur connue en quatre parties, dont les six différences alternatives soient des quarréz parfaits. »

En appelant $4a$ la grandeur donnée, z, y, x, v les quatre parties, il pose $z - y = 4t^2$, $z - x = 4s^2$, $z - v = 4r^2$, d'où x, y, z et v en fonction de a, t, s, r . Le problème se ramène à une triple égalité, c'est-à-dire qu'il faut évaluer à des carrés $r^2 - t^2$, $r^2 - s^2$ et $s^2 - t^2$. PRESTET donne une solution à trois paramètres n, m, l . Posant $f = n^2 + m^2$, $g = n^2 - m^2$,

$$k = \frac{12n^5 + 4nm^4}{22n^4m^4 + m^8} - 7n^8,$$

$$t = \frac{8n^2m^{16}l - 128n^8m^{12}l - 304n^{10}m^8l + 448n^{14}m^4l - 24n^{18}l}{49n^{16} - 308n^{12}m^4 + 470n^8m^8 + 44n^4m^{12} + 1m^{16}}$$

ou $2kfgnl + k^2f^2l$, $s = n^{2l} - m^{2l} + t$, $r = n^{2l} + m^{2l} + t$, $z = a + t^2 + r^2 = s^2$, $y = a - 3t^2 + r^2 + s^2$, $x = a = t^2 + r^2 - 3s^2$, $v = a + t^2 - 3r^2 + s^2$.

Après la floraison du XVII^e siècle, où les exemples précédents montrent l'exubérance exagérée des calculs, l'Analyse diophantienne des nombres rationnels fut graduellement abandonnée. Les mathématiciens du XVIII^e siècle avaient d'autres problèmes plus importants à traiter. Cependant, EULER lui consacre encore une bonne partie de son *Algèbre*, 1770, dont la traduction française parue en 1774 contient de plus les importantes additions de LAGRANGE qui écrit dans son avertissement : « Cette branche de l'Analyse a été presque abandonnée dans ce siècle ; et si on en excepte M. EULER, je ne connais personne qui s'y soit appliqué ; mais les belles et nombreuses découvertes que ce grand géomètre y a faites nous ont bien dédommagé de l'espèce d'indifférence que les autres géomètres paraissent avoir eue jusqu'ici pour ces sortes de recherches. Les commentaires de Pétersbourg sont pleins des travaux de M. EULER dans ce genre, et l'ouvrage qu'il vient de donner est un nouveau service qu'il rend aux amateurs de l'Analyse de DIOPHANTE. On n'avait point encore d'ouvrage où cette science fût traitée d'une manière méthodique, et qui renfermât et expliquât clairement les principales règles connues jusqu'ici pour la solution des problèmes indéterminés. Le traité précédent réunit ce double avantage... »

Nous avons cru devoir nous étendre un peu sur cette partie actuellement à peu près délaissée des Mathématiques. C'est que, du XVI^e à la fin du XVII^e siècle, elle a joué un rôle de premier plan, et qu'en l'oubliant on fausse la perspective de l'histoire. Elle a habitué les mathématiciens au calcul algébrique, et contribué ainsi au progrès général de notre science, facilitant en particulier la naissance des nouveaux calculs différentiel et intégral. D'autre part, comme nous allons le voir, elle a donné naissance à l'Analyse indéterminée des nombres entiers, qui porte aujourd'hui son nom même d'Analyse Diophantienne, et à la Théorie des Nombres.

La théorie des nombres et l'analyse diophantienne

Au XVII^e siècle, la théorie des nombres est née de l'étude même de l'œuvre de DIOPHANTE. C'est l'éditeur de cette œuvre, BACHET de Méziriac, qui étudie systématiquement les équations indéterminées du premier degré, principalement dans la seconde édition de ses *Problèmes délectables*, de 1624. En utilisant l'algorithme d'EUCLIDE, il démontre que deux nombres étant premiers entre eux, on peut trouver des multiples de ces nombres qui diffèrent entre eux de l'unité, ce qui lui permet de donner la solution générale en nombres entiers de l'équation $ax + by = c$. Des problèmes analogues avaient déjà été traités aux Indes par ARYABHATA et BRAHMAGUPTA, en Occident par LÉONARD DE PISE, REGIOMONTANUS, TARTAGLIA, mais BACHET a un souci de la rigueur qu'il serait vain de chercher avant lui dans ce domaine, sauf chez son modèle constant, EUCLIDE.

Le Père MERSENNE souleva la question des nombres parfaits, multiples et sous-multiples, ce qui amena des recherches dans ce domaine, de DESCARTES et de FERMAT en particulier. L'étude des nombres parfaits n'avait pas cessé d'intéresser les mathématiciens, mais ils étaient arrêtés par la recherche des nombres premiers de la forme $2^p - 1$, et les listes de nombres parfaits que l'on trouve chez les auteurs du xvi^e siècle sont toutes fautives. STIFEL, par ailleurs, avait indiqué le nombre des diviseurs d'un nombre donné, mais cet ensemble de recherches, y compris celles de DESCARTES et de FERMAT, relèvent beaucoup plus de l'Algèbre et de l'Analyse combinatoire que de la théorie des nombres proprement dite. C'est ainsi que FERMAT trouve vers 1636 la règle pour les nombres sous-doubles : si n et P premier satisfont à la relation $2^n - 1 = P(2^{n-3} + 1)$, le nombre $3P \times 2^{n-1}$ est sous-double, c'est-à-dire égal à la moitié de la somme de ses diviseurs, lui-même étant exclu de cette somme. Il croit que la règle donnera une infinité de nombres sous-doubles. En 1638, DESCARTES déclare avec raison qu'elle ne peut en donner que deux, P ne pouvant prendre que les valeurs 5 et 7.

FERMAT et DESCARTES donnent la règle de TABIT BEN KORAH (ix^e siècle), pour la formation de couples de nombres amiables, c'est-à-dire tels que chacun d'eux égale la somme des diviseurs de l'autre ; si $R = 3 \cdot 2^{n-1} - 1$, $S = 3 \cdot 2^n - 1$, $P = 9 \cdot 2^{n-1} - 1$ sont trois nombres premiers, les deux nombres $2nP$ et $2nRS$ sont amiables. Vers la même époque, les deux savants fabriquent à plaisir des nombres sous-multiples, ainsi que leurs émules SAINTE-CROIX et FRÉNICLE. C'est ainsi que DESCARTES donne le sous-double 1476304896, et indique des règles comme : « Tout sous-double divisible par 3, sans l'être par 7, 9, ni 13, multiplié par 273, donne un sous-triple. »

Mais ces amusements ne vont pas très loin. Ce ne sont que d'habiles combinaisons algébriques qui impliquent la connaissance de la somme des diviseurs d'un nombre décomposé en ses facteurs premiers, mais n'ont rien à voir avec la vraie théorie des nombres, que FERMAT va créer sur ces entrefaites.

Lorsque commence sa correspondance, en 1636, il est à peu près ignorant de tout en la matière. Et, cependant, nous le voyons, dès 1639, essayer le savoir de ses émules, comme FRÉNICLE, en leur proposant des problèmes qu'il sait impossibles, comme « trouver un triangle rectangle duquel l'aire soit un nombre carré, trouver deux carrés carrés desquels la somme soit carrée carrée, trouver quatre carrés en proportion arithmétique continue, trouver deux cubes desquels la somme soit cube ».

En 1640, il est en possession des plus importantes de ses découvertes et de ses méthodes. Il sait que $a^{p-1} \equiv 1 \pmod{p}$ pour p premier, a non divisible par p . Il a montré que $2^{27} - 1$ n'est pas premier, mais admet le facteur 223, et établi que tout nombre premier de la forme $4k + 1$ est d'une seule façon somme de deux carrés, et il possède sa méthode de démonstration par la descente infinie.

Il résumera dans une lettre à CARCAVI, d'août 1659, l'ensemble de ses découvertes : « J'appelai cette manière de démontrer la descente infinie ou indéfinie... ; je ne m'en servis en commencement que pour démontrer les propositions négatives comme, par exemple :

« Qu'il n'y a aucun nombre, moindre de l'unité qu'un multiple de 3, qui soit composé d'un carré et du triple d'un autre carré.

« Qu'il n'y a aucun triangle en nombres dont l'aire soit un nombre carré. »

Interrompons ici cette citation pour donner, au sujet de cette dernière affirmation, la traduction française de l'Observation sur DIOPHANTE où FERMAT traite la même question.

« Si l'aire d'un triangle était un carré, il y aurait deux bicarrés dont la différence serait un carré ; il s'ensuit qu'on aurait également deux carrés dont la somme et la différence seraient des carrés. Par conséquent, on aurait un nombre carré, somme d'un carré et du double d'un carré, avec la condition que la somme des deux carrés, qui servent à le composer, soit également un carré. Mais si un nombre carré est somme d'un carré et du double d'un carré, sa racine est également somme d'un carré et du double d'un carré, ce que je puis prouver sans difficulté. On conclura de là que cette racine est la somme des deux côtés de l'angle droit d'un triangle rectangle, dont l'un des carrés composants formera la base, et le double de l'autre carré la hauteur.

« Ce triangle rectangle sera donc formé par deux nombres carrés, dont la somme et la différence seront des carrés. Mais on prouvera que chacun de ces deux carrés est plus petit que les deux premiers, dont on a également supposé que la somme et la différence soient des carrés. Donc, si on donne deux carrés dont la somme et la différence soient des carrés, on donne par là-même, en nombres entiers, deux carrés jouissant de la même propriété et inférieurs.

« Par le même raisonnement, on trouvera toujours des nombres entiers de plus en plus petits satisfaisant aux mêmes conditions. Mais cela est impossible, puisqu'un nombre entier étant donné, il peut y avoir une infinité de nombres entiers plus petits. »

(On sait qu'un triangle rectangle en nombre, dont les côtés sont premiers entre eux dans leur ensemble, ont pour côtés $2mn$, $m^2 - n^2$ et $m^2 + n^2$, m et n premiers entre eux, de parités différentes ; on trouve déjà dans EUCLIDE X, comme 2 à la prop. 28, une relation analogue. L'aire est donc $mn(m^2 - n^2)$. Si elle est un carré parfait, m et n sont carrés, ainsi que $m^2 - n^2$. Soient $m = x^2$, $n = y^2$; x^4 est un carré, d'où $x^2 - y^2 = t^2$. $x^2 + y^2 = z^2$, ou encore $z^2 = t^2 + 2y^2$, $x^2 = t^2 + y^2$. Mais si $z^2 = t^2 + 2y^2$, $(z - t)(z + t) = 2y^2$, d'où $z - t = 4u^2$, $z + t = 2v^2$, et $z = v^2 + 2u^2$, $t = v^2 - 2u^2$, $y = 2uv$, $x^2 = v^4 + 4u^4$. Donc v^2 et $2u^2$ sont les côtés de l'angle droit d'un triangle rectangle dont l'aire v^2u^2 est un carré. Chacun de ces côtés est inférieur à z ...).

« Je fus longtemps, écrit FERMAT dans sa lettre à CARCAVI, sans pouvoir appliquer ma méthode aux questions affirmatives... De sorte que lorsqu'il me fallut démontrer que tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux carrés, je me trouvais en belle peine. Mais, enfin, une méditation diverses fois répétée me donna les lumières qui me manquaient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il fallut joindre par nécessité...

« Il y a infinies questions de cette espèce, mais il y en a quelques autres qui demandent des nouveaux principes pour y appliquer la descente... Telle est la question suivante : Tout nombre est carré ou composé de deux, de trois ou de quatre carrés. (Il avait énoncé cette proposition plus généralement, dans une lettre datée à tort, dans les Œuvres Complètes, de septembre ou octobre 1636, mais qu'il faut reporter à mai ou juin 1638). Tout nombre est la somme de trois nombres triangulaires au plus, ou de quatre carrés, ou de cinq pentagones, de six hexagones, sept heptagones, etc...

« Celle que j'avais proposée à M. FRÉNICLE et autres (WALLIS, LORD Brouncker) est d'aussi grande et même plus grande difficulté : Tout nombre non carré est de telle nature qu'il y a infinis carrés qui, multipliant ledit nombre, font un carré moins 1. Je la démontre par la descente appliquée d'une manière toute particulière. (Il s'agit de l'équation dite à tort, depuis EULER, équation de PELL : $ax^2 + 1 = y^2$).

« J'ai ensuite considéré certaines questions qui, bien que négatives, ne restent pas de recevoir très grande difficulté, la méthode pour y pratiquer la descente étant tout à fait diverse que les précédentes, comme il sera aisé d'éprouver. Telles sont les suivantes : Il n'y a aucun cube divisible en deux cubes. Il n'y a qu'un carré en entiers qui, augmenté du binaire, fasse un cube. Ledit carré est 25.

« Il n'y a que deux carrés en entiers, lesquels, augmentés de 4, fassent un cube. Lesdits carrés sont 4 et 121.

« Toutes les puissances carrées de 2, augmentées de l'unité, sont nombres premiers... » Cette dernière proposition, que FERMAT n'a cessé d'énoncer tantôt dubitativement, tantôt comme ici, et vers la fin de sa carrière seulement, d'une façon absolue, et qui porte sur les nombres $2^{2^n} + 1$, est fausse, comme EULER l'a vérifié pour $2^{32} + 1$ divisible par 641. Il est curieux de constater ici l'obstination de FERMAT, d'autant plus étrange qu'il avait effectué la factorisation aussi difficile de $2^{37} - 1$. Tant une conviction profonde, ou un préjugé d'inventeur, peuvent être un obstacle insurmontable.

Mais ce qui frappera le plus dans la Correspondance de FERMAT, c'est que l'on n'y rencontre jamais son grand théorème sur l'impossibilité de l'équation $x^n + y^n = z^n$ pour $n > 2$. Seuls y figurent les deux cas particuliers $n = 3$ et $n = 4$. Il y a là une forte présomption pour croire qu'effectivement, il n'avait pas de méthode pour démontrer le cas général, sa descente infinie devenant impuissante, dès $n = 5$. C'est dans ses remarques sur DIOPHANTE, notes personnelles écrites en marge de son exemplaire, pieusement recueillies et publiées par son fils en 1670, que la proposition est affirmée. Voici la traduction de sa remarque à la proposition 8 du livre II ; trouver deux carrés dont la somme soit un carré : « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré ; j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. » Les mathématiciens doivent être reconnaissants à Samuel FERMAT de son indiscrétion. La publication de cette note personnelle, que son père n'avait jamais voulu rendre publique, a

été un des principaux stimulants pour les théoriciens du nombre, et nous lui devons la plupart des grands progrès accomplis dans ce domaine.

Au XVIII^e siècle, l'œuvre de FERMAT est reprise principalement par EULER, LAGRANGE, LEGENDRE et GAUSS.

EULER publia en 1736 la première démonstration du théorème de FERMAT affirmant que $x^{p-1} - 1$ est divisible par p , si ce nombre p est premier et ne divise pas x . Il généralisera d'ailleurs la proposition en 1760 en introduisant la fonction $\phi(n)$ ou indicateur de n . L'indicateur est égal au nombre des entiers inférieurs à n et premiers avec lui. En 1770, WARING énonçait un théorème qu'il attribuait à John WILSON : si p est premier, $1 + (p-1)!$ est divisible par p . LEIBNIZ, dans un de ses manuscrits, avait déjà énoncé cette proposition, dont LAGRANGE publia une preuve en 1773, en remarquant de plus que la proposition réciproque est vraie.

Le problème des partitions fut attaqué pour la première fois par EULER en 1741, qui discuta la question de trouver le nombre de façons de décomposer un nombre donné en une somme de n termes, n donné, soit que les termes soient tous inégaux, soit que certains soient égaux entre eux. Il reprit la question en 1748 dans son *Introductio in Analysin Infinitorum*. Entre 1773 et 1782, il s'occupa de triangles dont les côtés et les médianes sont rationnels, et, pendant quarante années, il s'intéressa à l'affirmation de FERMAT et de BACHET, suivant laquelle tout nombre est la somme de quatre carrés au plus. Ce n'est que vingt ans après ses premières recherches sur la question qu'il publia, en 1751, quelques résultats importants, en particulier sa formule qui exprime le produit de deux sommes de quatre carrés sous une forme analogue :

$$(a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2) = x^2 + y^2 + z^2 + v^2,$$

avec $x = ap + bq + cr + ds$, $y = aq - bp \pm cs \mp dr$,

$$z = ar \mp bs - cp \pm dq, \quad v = as \pm br \mp cq - dp.$$

La première preuve publiée fut celle de LAGRANGE en 1772, où l'auteur reconnaissait tout ce qu'il devait à la publication précédente d'EULER. Celui-ci publiait à son tour, l'année suivante, une preuve plus simple que celle de LAGRANGE, et qui n'a pas été dépassée depuis.

L'équation, dite de PELL, $x^2 - Ay^2 = 1$, où les lettres représentent des entiers, est née, comme nous l'avons vu, tout au moins aux temps modernes, du défi porté par FERMAT aux mathématiciens anglais. WALLIS et BROUNCKER trouvèrent une méthode permettant de découvrir les racines lorsqu'elles existent, mais n'en établissant pas l'existence.

Cette méthode, comme celle de BACHET pour les équations indéterminées du premier degré, revient en dernière analyse à l'Algorithme d'EUCLIDE, ou si l'on préfère, à celui des fractions continues. En 1765, EULER expose la méthode des mathématiciens anglais d'une façon plus claire en utilisant la fraction continue qui exprime $\sqrt{A}$, et trouve plusieurs faits importants. Un an ou deux après, toujours au moyen du même algorithme, LAGRANGE prouve l'existence des racines. L'importance de l'équation de PELL réside dans le fait que toute équation indéterminée du second degré se ramène à elle. EULER a résolu un grand nombre d'équations indéterminées. A la suite de FERMAT, il a étudié quelques-unes des plus simples formes quadratiques, et il a donné une preuve de l'impossibilité de l'équation $x^3 + y^3 = z^3$, en nombres entiers.

Il se présente en somme, en théorie des nombres, comme le brillant continuateur de l'œuvre du grand mathématicien français.

Nous venons de citer plusieurs fois le nom de LAGRANGE.

Ici, comme dans bien d'autres branches de l'Analyse, ce disciple d'EULER entre plusieurs fois en compétition avec son maître, chacun d'eux travaillant à partir de résultats obtenus par l'autre, tantôt en simplifiant les preuves, tantôt en déduisant de nouveaux résultats.

En plus de ses travaux déjà cités, LAGRANGE a montré qu'une congruence de module premier a un nombre de racines au plus égal à son degré. Surtout, en 1773, il fit les premières recherches générales sur les formes quadratiques binaires.

LEGENDRE s'intéressa en 1785 aux congruences binômes. Pour p premier, il prouva qu'il y a exactement $\Phi(e)$ nombres appartenant à l'exposant e , si e divise $p - 1$, ce qui signifie qu'un de ces nombres satisfait à la congruence $a^e - 1 = 0 \pmod{p}$, mais ne satisfait à aucune congruence $a^m - 1 = 0 \pmod{p}$ où $m < e$. Il donna en 1808 une preuve insuffisante de l'existence d'une infinité de nombres premiers dans toute progression arithmétique $a + nb$, où a et b sont premiers entre eux. C'est DIRICHLET qui devait, en 1837, prouver définitivement cette proposition. En 1798, LEGENDRE donnait une expression du nombre de décomposition d'un entier en somme de deux carrés et établissait que tout nombre qui n'appartient ni à la forme $8n + 7$, ni à la forme $3n$ est la somme de trois carrés. GAUSS devait, en 1801, apporter une preuve plus claire de ce fait. CAUCHY ayant réussi en 1813, 1815 à établir la proposition de FERMAT : Tout nombre est la somme de m nombres polygones de m côtés, LEGENDRE simplifia immédiatement la preuve de CAUCHY et montra que tout nombre suffisamment grand est la somme de quatre ou cinq polygones de m côtés, selon que m est impair ou pair.

Il déduisit de formules de son traité de 1828, sur les fonctions elliptiques, que le nombre de façons dans lesquelles un nombre N est la somme de quatre triangulaires est égal à la somme des diviseurs de $2N + 1$, et trouva le nombre de façons dans lesquelles N est la somme de huit triangulaires.

En 1828-29, JACOBI comparait deux séries infinies de la même fonction elliptique pour montrer que, si p est impair et si $s(p)$ est la somme de ses diviseurs, le nombre des représentations de $2ap$ comme somme de quatre carrés est $8s(p)$ ou $24s(p)$ selon que $a = 0$ ou > 0 . D'une façon analogue, LEGENDRE et lui-même prouvèrent simultanément qu'il y a exactement $s(p)$ groupes de quatre nombres impairs dont la somme est $4p$. On doit encore à LEGENDRE le premier énoncé, en 1785, de la loi de réciprocité des résidus quadratiques. Sa première démonstration de cette loi était d'ailleurs incomplète. GAUSS en donna ensuite six preuves exactes. Les travaux arithmétiques de LEGENDRE ont porté surtout sur les formes quadratiques. Ils ont donné lieu principalement à ses *Recherches d'analyse indéterminées* en 1785, son *Essai sur la théorie des nombres* en 1798, réédité en 1808, et sa *Théorie des Nombres* parue en 1830.

Le dernier grand nom à signaler en Théorie des Nombres à la fin du XVIII^e siècle est celui de GAUSS. Il écrit lui-même dans la préface de ses *Disquisitiones Arithmeticae*, parues en 1801 et traduites en français par

POULLET-DELISLE : « ...Lorsqu'en 1795 (il avait alors 18 ans), j'ai commencé à m'appliquer à ce genre de considérations, je n'avais absolument aucune idée de tout ce qui avait été fait sur ce sujet, même par les modernes, et... j'étais privé de tous les secours que j'aurais pu tirer de leurs travaux. Occupé dans ce temps d'une autre matière, je tombai par hasard sur une vérité importante de l'Arithmétique (— 1 est résidu de tous les nombres premiers de la forme $4n + 1$, et non résidu de tous les nombres premiers de la forme $4n + 3$, autrement dit l'équation $x^2 + 1 = py$, où p est premier, est possible ou non en nombres entiers selon que p est un multiple de 4 plus ou moins 1) ; comme elle me sembla très belle par elle-même, et que je la soupçonnais liée à d'autres plus importantes, j'employai toute la contention d'esprit dont j'étais susceptible à découvrir les principes sur lesquels elle s'appuyait, et à en trouver une démonstration rigoureuse ; le succès ayant répondu à mes vœux, je me sentis tellement entraîné par l'attrait de ces questions, qu'il me fut impossible de les abandonner, et, comme une vérité me conduisait à une autre, la plus grande partie des quatre premières sections était déjà terminée avant que j'eusse rien vu des travaux des autres géomètres sur ce sujet. (Les quatre premières sections forment la théorie des congruences).

M'étant ensuite trouvé à même de lire les ouvrages de ces hommes de génie, je ne tardai pas à reconnaître que j'avais employé la plus grande partie de mes méditations à des choses faites depuis longtemps ; mais, animé d'une nouvelle ardeur, je m'efforçai, en suivant leurs pas, de cultiver plus avant le champ de l'Arithmétique, et telle a été l'origine des sections V, VI et VII (formes quadratiques et équations $z^n - 1 = 0$). »

Nous venons de donner un aperçu de l'histoire de la théorie des nombres que l'on pourrait appeler classique. Elle a été étudiée tout au long du XIX^e siècle et pendant le XX^e, mais les noms à citer seraient alors très nombreux.

Par ailleurs, déjà avec GAUSS, elle commence à subir une mutation qui conduira à la théorie des corps de nombres algébriques.

Jean ITARD.