Sur différents types de démonstrations rencontrées spécifiquement en arithmétique.

Martine Bühler et Anne Michel-Pajus
Groupe M. :A.T.H.
(Mathématiques : Approche par des Textes Historiques)
I.R.E.M. Paris 7

Un des aspects intéressants de l'arithmétique est que, sans avoir besoin d'un grand arsenal théorique, on peut y faire de véritables démonstrations mathématiques s'appuyant sur des raisonnements d'une certaine finesse et obtenir ainsi des résultats non triviaux.

Ces raisonnements, parce qu'ils portent sur les entiers, sont facilement accessibles par l'intuition. On les retrouve tout au long de l'histoire, mais sous des formes plus ou moins théorisées.

Le bagage théorique de base peut se limiter à une seule propriété, mais qui apparaît sous des formes différentes selon les points de vue et les cadres.

Tout ceci donne à l'arithmétique un caractère formateur spécifique.

I. 1. Un survol historique de travaux en arithmétique

Les considérations sur pair-impair, multiples, nombres premiers nous viennent probablement de l'école de Pythagore. Cependant, on ne possède aucun texte des Pythagoriciens. On connaît ce courant par l'œuvre du néopythagoricien Nicomaque de Gérase (II^ème^ siècle après J.-C.) qui a écrit une *Introduction Arithmétique*, dans laquelle on trouve des considérations sur pair-impair, nombres figurés, crible d'Eratosthène cité par Nicomaque. Nicomaque ne donne pas de démonstration, mais des exemples et des vérifications pour de petites valeurs.

La civilisation chinoise a laissé des travaux arithmétiques, dont le célèbre théorème des restes, dont le nom vient du problème 26 du chapitre 3 du *Sunzi Suanjing* (Manuel Mathématique du Maître Sun) datant environ du quatrième siècle de notre ère. On y trouve des règles de résolution sans explicitation des démonstrations.[1]

Les *Eléments* d'Euclide (III^ème^ siècle avant J.C.) restent une source importante sur les connaissances des Grecs en arithmétique. Ce traité est essentiellement géométrique, mais contient néanmoins trois livres consacrés à l'arithmétique, présentant des définitions et des propositions sur les nombres, soigneusement démontrées.

Diophante d'Alexandrie, dont on connaît peu de choses (il a vécu entre le II^ème^ siècle avant J.-C. et le IV^ème^ siècle après J.-C.), a écrit une œuvre originale. Ses *Arithmétiques* comportaient au départ 13 livres[2]. C'est un algébriste qui a traduit ces livres en arabe au X^ème^ siècle, ce qui explique la manière dont les arabes ont majoritairement lu Diophante et utilisé l'outil algébrique pour résoudre les problèmes diophantiens. Un autre courant, initié en particulier par al-Khazin a développé une arithmétique entière sans algèbre.

En Occident, l'arithmétique connaît un renouveau au XVII^ème^ siècle avec Fermat. Diophante, longtemps oublié en Occident, est redécouvert à la Renaissance par six des treize livres des *Arithmétiques*. Bombelli incorpore des problèmes de Diophante dans l'édition de *l'Algebra* de 1572. En Allemagne, à la même époque, Xylander publie une traduction en latin de Diophante (1575). Enfin, Bachet de Méziriac donne en 1621 une édition bilingue en grec et en latin de ces six livres retrouvés. C'est cette édition que lit et annote Fermat. Celui-ci n'a

[1] MARTZLOFF Jean-Claude, *Histoire des mathématiques chinoises,* Masson, 1987
[2] Voir *Mnémosyne* n°

jamais écrit de traité d'arithmétique et c'est dans sa correspondance qu'il faut chercher ses écrits en arithmétique.

Au XVIIIème siècle, Euler, qui s'intéresse à tous les domaines des mathématiques, publie dans les *Commentaires de Petersbourg* un certain nombre de démonstrations de résultats énoncés par Fermat.

Au XIXème siècle, l'intérêt pour l'arithmétique est renouvelé par les travaux de Lagrange, Legendre et Gauss.

I.2. Nos outils d'analyse

En examinant les arguments de divisibilité, on s'aperçoit que les auteurs utilisent, explicitement ou non, un des quatre résultats fondamentaux (équivalents entre eux) suivants :

- « Proposition 32 d'Euclide » dite « Lemme d'Euclide » : [LE1] : si un nombre premier divise un produit, alors il divise l'un des facteurs du produit.[3]. On le rencontre aussi sous sa forme contraposée [LE2] : si un nombre premier *p* ne divise ni *a* ni *b*, alors il ne divise pas le produit *ab*.
- « Proposition (26) d'Euclide » [PE] : si deux nombres *a* et *b* sont premiers avec *p*, le produit *ab* sera aussi premier avec *p*.
- « Théorème de Gauss » [TG] : si un nombre divise un produit et est premier avec l'un des facteurs du produit, alors il divise l'autre.
- « Théorème fondamental de l'Arithmétique » [TF] : la décomposition d'un nombre entier en facteurs premiers est unique.

Il est alors intéressant de se demander lesquels de ces quatre résultats sont utilisés et/ou explicités et/ou démontrés dans les textes, de regarder leur ordre d'exposition, la façon dont ils apparaissent liés. Nous n'avons fait ce travail que pour quelques traités mais cette recherche suffit à montrer les différents points de vue des auteurs et leurs priorités.

Nous avons aussi tenté une classification sommaire des méthodes de raisonnements, visibles à travers l'organisation des démonstrations

- <u>Méthodes de tiroirs.</u>
  - [PT] : Utilisation d'un nombre fini de tiroirs pour ranger des objets en nombre strictement supérieur : il y a donc au moins un tiroir contenant au moins deux objets. C'est le « principe des tiroirs » (pigeonholes) ou « principe de Dirichlet ».
  - [DC] : Partition des situations étudiées en un nombre fini de cas qu'on examine exhaustivement. C'est la méthode de « disjonction des cas ».
  - [Bi] : Mise en bijection de deux ensembles finis de même cardinal.

- <u>Méthodes d'escalier</u>.
  - [DF] : Descente finie jusqu'à un entier convenable fournissant la conclusion soit directement soit par l'absurde.
  - [DI] : Descente qui porte en elle-même sa contradiction parce qu'elle construit une suite infinie strictement décroissante d'entiers positifs. C'est la « méthode de descente infinie » de Fermat.
  - [MS] : Induction simple : on démontre le passage d'un entier particulier spécifié au suivant et cet exemple générique justifie la généralisation.
  - [MR] : Raisonnement par récurrence théorisé.

---

[3] La numérotation est celle de la traduction de Peyrard (voir bibliographie).Les propsitions 26 et 32 dont il est question ici figurent dans le livre VII.

- [PPE] : Raisonnement utilisant le plus petit élément d’une partie non vide de N.

L’atelier s’est déroulé en deux séances pendant lesquelles nous avons étudié deux groupements de textes permettent d’illustrer ce qui précède. Le premier groupement comportait des textes d’Euler, de Legendre, Gauss et Jules Tannery, et permettait d’examiner l’utilisation des résultats fondamentaux, le lien entre eux, ainsi que leur apparition dans les traités de théorie des nombres. Le deuxième groupement était centré sur les méthodes d’escalier, avec des textes d’Euclide, Fermat, Legendre et Tannery.

Ces textes sont présentés et étudiés dans un article plus complet qui paraîtra en septembre 2006 dans la revue *Mnémosyne* éditée par le groupe M. :A.T.H. de l’I.R.E .M. Paris 7. Ce travail est le fruit de recherches menées par le groupe à l’I.R.E.M. et entre dans le cadre d’un projet de recherche de l’I.N.R.P., qui donnera lieu à publication.