COMPTE RENDU D'ATELIER

V.Battie – IREM de Lyon

CONSTRUCTION DE PREUVES DANS L'HISTOIRE : EXPLOITATION DE TEXTES HISTORIQUES EN CLASSE DE TERMINALE S SUR LE THEOREME FONDAMENTAL DE L'ARITHMETIQUE.

Atelier animé par **VERONIQUE BATTIE – IREM DE LYON**

Résumé de présentation avant les journées : Nous proposerons aux participants d'étudier des textes d'Euclide et Gauss sur la factorisation unique des entiers que nous avons utilisés lors de nos interventions dans des lycées (groupe « Un chercheur dans la classe ! » de l'IREM de Lyon) et les productions de différents groupes d'élèves (écrits et extraits de transcriptions de leurs recherches). A partir de nos travaux en didactique de l'arithmétique (LEPS – LIRDHIST[1]), nous présenterons en guise de synthèse une analyse épistémologique et didactique de cette exploitation en classe de textes historiques.

1. OBJECTIFS DE L'ATELIER

Au-delà de notre souhait de faire vivre un vrai moment d'atelier, en particulier en permettant aux participants de travailler sur des documents et en permettant autant que possible un réel échange entre tous (y compris l'animatrice !), les objectifs étaient les suivants :

- Présenter un exemple d'intervention du groupe « Un chercheur dans la classe ! » de l'IREM de Lyon
- Illustrer une façon d'exploiter des textes historiques en classe de mathématiques pour travailler sur le raisonnement mathématique via la production de preuves (exploitation didactique du décalage culturel en jeu.
- Présenter nos travaux en didactique de l'arithmétique (au sens théorie élémentaire des nombres (ici entiers)) sur un exemple préalablement regardé par les participants

2. DEROULEMENT EFFECTIF DE L'ATELIER

- 1er temps : introduction par l'animatrice avec données des consignes pour le travail en groupes (environ 10 mn)
- 2ème temps : travail en groupes de 3 à 5 participants (environ 40 mn). Le temps a manqué pour cette partie : les participants n'ont pas eu suffisamment de temps pour étudier dans le détail les documents fournis et suivre entièrement les consignes proposées. Une conséquence a été que la plupart des groupes n'a pas pu mettre par écrit (transparents vierges mis à leur disposition en vue de la mise en commun) le fruit de leurs échanges.
- 3ème temps : mise en commun pour discussion (environ 20 mn)
- 4ème temps : quelques éléments de synthèse de l'animatrice (environ 20 mn)

3. INTRODUCTION DE L'ATELIER ET CONSIGNES DONNEES AUX PARTICIPANTS

Au sein de l'IREM de Lyon, le groupe « Un chercheur dans la classe » a pour principal objectif de donner aux élèves de lycée une image des mathématiques comme science vivante grâce à des interventions de chercheurs dans leurs classes. Les visites prennent différentes formes : conférences, débats, travaux en groupes pour les élèves. Dans ce contexte, nous avons proposé à une classe de terminale scientifique (enseignement de spécialité) de démontrer le théorème fondamental de l'arithmétique[2] (existence et unicité d'une décomposition en produit de nombres premiers pour tout entier égal ou supérieur à 2) à partir de la proposition 31 du livre VII des Eléments d'Euclide (1994) et du théorème 16 de la Section Seconde des Recherches Arithmétiques de Gauss (1953). D'après Bühler & Michel-Pajus (2007) et Goldstein (1992), on peut considérer que ces textes représentent

[1] EA 4148, Laboratoire d'Etudes du Phénomène Scientifique, équipe LIRDHIST (Lyon1 : Institut de Recherche en Didactiques et en HIstoire des Sciences et des Techniques).
[2] Noté TFA dans la suite du texte.

respectivement les premiers éléments de preuve de la partie existence du TFA et la première démonstration de la partie unicité[3]. La séance a duré deux heures et a été découpée en deux temps : nous avons proposé aux élèves de travailler en groupes sur le texte d'Euclide puis, après une mise en commun, dans un second temps sur le texte de Gauss après une introduction mathématique de notre part.

Nous avons fourni aux participants de l'atelier APMEP les documents donnés aux élèves ainsi que des productions écrites finales de différents groupes d'élèves (différents lycées de Lyon). Les documents communs à tous les groupes de participants de l'atelier sont donnés en annexe. Nous leur avons aussi fourni le programme d'arithmétique de terminale S (enseignement de spécialité). Les consignes proposées aux 5 groupes ont été les suivantes :

1. Faire une analyse mathématique des deux preuves historiques
2. Idem avec les preuves des élèves (en écho à l'analyse faite en 1.)

Pour la mise en commun : communiquer les éléments-clefs de votre méthodologie d'analyse et de vos résultats côté élèves.
Horaire pour la mise en commun : …
Répartition des productions d'élèves :

- Groupe 1 : groupes 1 et 2 + classe A n°1
- Groupe 1 : groupes 1 et 2 + classe A n°2
- Groupe 1 : groupes 1 et 2 + classe A n°3
- Groupe 1 : groupes 1 et 2 + classe A n°4
- Groupe 1 : groupes 1 et 2 + classe A n°5

4. ELEMENTS DE L'EXPOSE DE SYNTHESE

Le court exposé était relatif à la fois aux productions écrites finales des groupes 1 et 2 d'élèves (cf. annexe) étudiées par tous les groupes de participants et à la transcription des échanges au sein des groupes d'élèves (transcription qui a été distribuée aux participants à la fin de l'atelier (et non en cours de l'atelier pour limiter le corpus en jeu pour des raisons de temps)). Cet exposé renvoyait principalement à l'une de nos publications à paraître (Battie, 2009).

➢ DIMENSIONS ORGANISATRICE ET OPERATOIRE DANS LE RAISONNEMENT EN ARITHMETIQUE

Dans le raisonnement en arithmétique, nous distinguons deux dimensions qui interagissent.

La dimension organisatrice s'identifie au raisonnement global qui organise et structure les différentes étapes (on pourrait parler du « squelette » de la démonstration). Par exemple, outre les figures usuelles du raisonnement mathématique, en particulier le raisonnement par l'absurde, on identifie au niveau de la composante organisatrice le raisonnement par récurrence (et autres formes d'exploitation dans le raisonnement de la propriété de bon ordre de l'ensemble N), la disjonction de cas et la recherche exhaustive avec l'idée de ramener la résolution d'un problème à l'étude d'un nombre fini de cas, le jeu d'extension-réduction (méthode spécifique aux anneaux factoriels) et le principe local-global.

La dimension opératoire correspond quant à elle à tout ce qui relève des manipulations calculatoires (au sens le plus large) qui sont opérées sur les objets en jeu et qui permettent la mise en oeuvre des différentes étapes de la dimension organisatrice. Nous identifions par exemple les formes de représentation choisies pour les objets, l'utilisation de théorèmes-clefs, les manipulations de nature algébrique et l'ensemble des traitements opératoires relevant de l'articulation entre la structure d'anneau de $(Z,+,\times)$ et celle d'ensemble bien ordonné de $(N, \leq)$ relative aux deux ordres divisibilité et ordre naturel.

➢ PARTIE EXISTENCE DU TFA

[3] Lors de notre atelier, nous avons oublié de mentionner l'article de Michel Henry (2001). Nous profitons de ce compte-rendu pour combler cet oubli…

COMPTE RENDU D'ATELIER
V.Battie – IREM de Lyon

La représentation des trois nombres A, B et C via des segments de droite ainsi regroupés dans le texte d'Euclide favorise selon nous une lecture en termes de relation d'ordre naturel : A est plus grand que B, qui est lui-même plus grand que C. Et c'est cet ordre-là qui est essentiel pour la dimension organisatrice de la preuve : le raisonnement suivi par Euclide est un raisonnement indirect, par l'absurde, exploitant la propriété que toute suite strictement décroissante d'entiers naturels est finie. Et, du côté de la dimension opératoire, c'est la relation d'ordre divisibilité qui prime et en particulier la transitivité de cette relation. La correspondance entre l'ensemble des trois segments A, B et C et les trois nombres A, B et C intervenant dans le texte de la preuve permet de mettre en valeur l'articulation entre la structure d'anneau de $(Z,+,\times)$ et celle d'ensemble bien ordonné $(N,\leq)$ relative aux deux ordres divisibilité et ordre naturel : B mesure A et B est plus petit que A, C mesure B et C plus petit que B. Cette articulation, très insuffisamment mise en valeur dans l'enseignement, est ici essentielle et coïncide avec celle existant entre dimensions organisatrice et opératoire. Comme nous l'avons souligné dans la première partie de l'article, la présence d'une disjonction des cas premier et composé rencontrée du côté de la dimension organisatrice est liée à l'énoncé de la proposition VI.31 qui nous renseigne spécifiquement sur le cas composé. Comme le souligne Samuel (1967), pour démontrer l'existence d'un diviseur premier pour tout entier plus grand que 1 il n'y a pas besoin de séparer les cas premier et non premier. C'est la prise en compte du contexte culturel associé à la proposition VII.31 (et VII.32) qui légitime la mise en valeur de cette disjonction de cas. Avec l'énoncé et la preuve de cette proposition d'Euclide, nous avons les éléments-clefs, pour démontrer la partie existence du TFA: la proposition 31 du côté opératoire et le raisonnement indirect, par l'absurde, exploitant la propriété que toute suite strictement décroissante d'entiers naturels est finie pour l'élaboration de la dimension organisatrice.

Du côté élèves, nous nous sommes intéressés dans un premier temps aux productions écrites finales. Nous disposons d'une preuve de la proposition 31 pour les deux groupes et d'une preuve pour la partie existence du TFA uniquement pour le groupe 2. Du côté de la dimension opératoire, on constate que la transitivité de la relation d'ordre divisibilité est explicitée par les deux groupes dans l'écriture d'une preuve de la proposition 31. Pour le groupe 2, cet élément clef est écrit en premier et il est particulièrement bien mis en valeur. Pour ce qui est de la dimension organisatrice, ils ont adopté un raisonnement direct sans justifier que la démarche amorcée se termine : « [...] et ainsi de suite. » écrit le groupe 1, «[...] et on retrouve nos deux possibilités pour C. » conclue le groupe 2. Ce dernier fait de même pour sa preuve de la partie existence du TFA : « [...] et on reprend les étapes précédentes pour C. ». La spécificité des nombres en jeu est mentionnée une fois par le groupe 1 au début de sa preuve (« soit $A\in N$ ») et une fois par le groupe 2 dans sa deuxième preuve uniquement (« $A=kB$, $k\in N^*$ et $k\geq 2$ »). La relation d'ordre naturel existant entre les différents nombres intervenant dans leurs preuves n'est explicitée que par le groupe 2, une seule fois (« $A=kB$, $k\in N^*$ et $k\geq 2$. $B < A$. ») sans que cela soit repris. La deuxième preuve du groupe 2 exploite judicieusement le résultat de la proposition 31 et sa dimension organisatrice a les mêmes caractéristiques que celle de sa preuve de la proposition 31 : raisonnement direct sans justification du caractère fini de la démarche et disjonctions de cas mises en avant. Du côté de l'opératoire, la relation de divisibilité est traduite en termes de division euclidienne via le mot dividende en faisant la confusion entre dividende et quotient. Le symbole « $\mid$ » utilisé par convention pour exprimer la relation d'ordre divisibilité, et qui se lit divise, est semble-t-il employé par les élèves du groupe 2 en référence à la division euclidienne.

L'analyse de la recherche des élèves nous apporte de nouveaux éléments. Lors de notre exposé, nous avons souligné en premier lieu que ce qui n'est pas justifié par les élèves du côté de la dimension organisatrice dans leurs productions écrites apparaît dans leur recherche comme quelque chose de problématique. Dans le groupe 2, la contradiction soulevée par Euclide est questionnée :

Je vois par pourquoi c'est pas possible dans les nombres que chacun serait plus petit que le précédent.
Parce que t'as forcément un moment.
Non mais à l'époque grecque ils ne considéraient pas encore les nombres négatifs.
Quand tu arriveras à 1 tu arriveras.
Tous les entiers naturels elle a dit donc ouais on peut supposer que pour eux les négatifs ça

existe pas.
Ouais.
ça paraîtrait absurde pour eux de mesurer quelque chose de négatif.
Ouais mais c'est pas ça si tu divises chaque fois un nombre par un nombre plus petit c'est pas un négatif mais ça tend vers 0 mais ils avaient pas inventé les nombres à virgule c'est ça ?
Ouais je pense pas.
Ouais ils avaient pas vu les décimaux.
Extrait 2.2

Ce groupe règle donc le problème de la contradiction soulevée par Euclide en se référant au contexte mathématique historique et non aux besoins intrinsèques de la preuve développée.
Pour le groupe 1 quant à lui, le problème est soulevé :

Oui donc euh, parce que là on peut dire que C s'il est premier ça marche s'il est pas premier il est divisible par plusieurs, enfin j'sais pas il est divisible par d'autres nombres, et il faut montrer que c'est pas infini.
Faut partir avec un petit arbre, on part de A.
Faut montrer que cet arbre-là il est pas infini, qu'à un moment il s'arrête… Que tu ne peux pas le diviser indéfiniment quoi.
Extrait 1.6

Du côté opératoire, la transitivité de la relation d'ordre divisibilité est bien explicitée dans les productions écrites des deux groupes. L'analyse des échanges montre que les élèves sont particulièrement attentifs à cet élément de l'opératoire et cela dès le début de leurs recherches. Un élève du groupe 2 lui donne le statut de théorème : « Là j'ai l'impression qu'on est en train de revoir le théorème si a divise b et si b divise c alors a divise c. ». Le mot transitivité sera ensuite mentionné. Pendant la première demi heure de la recherche du groupe 1, avant que nous clarifions la consigne en jeu auprès de lui, une partie de ce groupe pense que la première consigne renvoie exclusivement à l'énoncé de la proposition 31. Dans ce contexte, ce que retiennent certains élèves de cette proposition c'est la relation de transitivité :

En gros c'qui dit Euclide c'est que si B divise A et C divise B alors A divise C c'est tout on va pas rentrer dans des raisonnements.
Oui mais on montre.
C'est la deuxième question, démontrer, elle dit écrire la preuve d'Euclide avec votre langage mathématique, c'est ça notre langage mathématique.
Extrait 1.3

L'assurance avec laquelle les élèves utilisent la transitivité et l'importance qu'ils lui accordent contrastent avec la fragilité avec laquelle ils évoluent lorsqu'ils tentent d'utiliser des pensées organisatrices rencontrées en classe. Comme nous l'avions montré dans le cas du théorème de Gauss (Battie, 2007), il y a un déséquilibre dans le travail des élèves en termes de contrôle des deux dimensions organisatrice et opératoire. Ce sont des éléments de la dimension opératoire (en particulier des théorèmes emblématiques de la culture d'enseignement concernée) qui guident prioritairement les élèves dans leur recherche. On en trouve d'ailleurs des traces dans les productions écrites. Nous avions en particulier observé que la transitivité était bien mise en valeur dans la preuve écrite du groupe 2 de la proposition 31, notamment à l'aide d'une numérotation. Lors de leurs échanges, le statut de cette numérotation est précisé: « ça c'est le 1, j'ai mis des étapes. ». Ce qui illustre clairement selon nous l'importance du rôle attribué par les élèves à ce théorème dans la démarche de preuve.
Du côté de l'opératoire à nouveau, nous avons souligné que les élèves du groupe 2 font référence à la division euclidienne :

Mais mais attend quand on notait ce symbole C divise A ça veut dire qu'il y avait pas de reste. Quand on mettait ce symbole là il n'y avait pas de reste?
Non
[…]
Si on voit la division euclidienne avec les restes là.
C'est simplement tu te souviens quand tu fais une division ben tu prends un grand nombre tu le divises par un autre, au début tu fais d'abord qu'avec un chiffre et puis tu les rajoutes au fur et à mesure. Par exemple on va prendre j'sais pas, 100 tu le divises par 5 tu vas d'abord prendre le premier nombre tu vas voir que ça fait 2 il va rester 0.
On fait sans reste quoi.
Ensuite il te reste 0, voilà, mais au début c'est vrai que t'as qu'un chiffre et donc ça te donne l'impression qu'il y a un reste en fait non c'est simplement que tu as fait la division.
Extrait 2.4

Dans cet extrait la relation de divisibilité est pensée en référence à la division euclidienne : elle correspond au cas particulier où le reste est nul. Le symbole « | » n'évoque pas spécifiquement aux élèves la relation d'ordre divisibilité. Ce symbole se lit « divise » et les élèves lui associent l'action diviser qui appelle un résultat, comme l'explique l'un d'eux qui se situe au niveau de la technique opératoire. Parmi les cinq expressions exprimant la relation de divisibilité entre deux entiers A et B (Zazkis, 2002), « A divise B » est la seule à qui est associé spécifiquement un symbole dont l'utilisation favorise naturellement cette expression par rapport aux autres. En classe de mathématiques, l'emploi de ce symbole peut être source de malentendus entre l'enseignant et les élèves si ces derniers n'utilisent pas ce symbole spécifiquement en référence à la relation divisibilité. Comme cela apparaît dans cet extrait, les élèves peuvent faire tout un détour masqué pour l'interpréter.

➢ PARTIE UNICITE DU TFA

La dimension organisatrice principale de la preuve de Gauss est un raisonnement par l'absurde mis en oeuvre en deux étapes définies par le changement d'objets sur lesquels on travaille. Le résultat à démontrer amène naturellement à travailler sur les entiers via des décompositions en produit de nombres premiers : dans la première étape du raisonnement par l'absurde, ce sont les nombres premiers qui sont objets du travail opératoire et, dans la deuxième, ce sont les exposants associés à ces nombres premiers qui le sont. Dans la première étape, la dimension organisatrice se complexifie avec un raisonnement par double inclusion (les deux ensembles de nombres premiers définissant respectivement chacune des deux décompositions considérées sont égaux) et dans chacune des inclusions à démontrer apparaît un raisonnement par l'absurde. La complexification de la dimension organisatrice associée à la double apparition d'un raisonnement par l'absurde a pour origine l'utilisation du lemme d'Euclide sous sa forme contraposée (n°14 dans le texte de Gauss). On simplifie la preuve de Gauss du point de vue de la dimension organisatrice en utilisant le lemme d'Euclide sous sa forme directe. Soulignons toute l'importance du lemme d'Euclide (sous sa forme contraposée ou non) pour établir le TFA : lemme d'Euclide et unicité d'une décomposition en produit de nombres premiers (partie fondamentale du TFA) sont équivalents. Dans la seconde étape de la preuve, la dimension organisatrice se complexifie aussi avec l'apparition d'un raisonnement par l'absurde qui contredit le résultat obtenu dans la première étape. Dans cette étape, l'élément-clef de la dimension opératoire est la division des décompositions en jeu par un diviseur commun judicieusement choisi.

Après avoir apporté ces éléments d'analyse de la preuve de Gauss, nous nous sommes intéressés tout d'abord aux productions écrites finales des deux groupes d'élèves étudiés par tous les groupes de participants. Dans les deux preuves de la partie unicité du TFA, le raisonnement par l'absurde principal et les deux étapes liées au changement d'objets sont explicitées. Pour la première étape, seul le résultat associé est donné par les deux groupes ; on ne trouve aucune trace du lemme d'Euclide, en particulier sous sa forme contraposée utilisée par Gauss. Pour la deuxième étape, un raisonnement par l'absurde apparaît via les notations adoptées. Seul le groupe 1 explicite la contradiction en référence à

la première étape. Nous avons ensuite zoomer sur un extrait de la transcription des discussions des élèves pour apporter de nouveaux éléments pour le groupe 1 :

Elève	Si je divise A par a^n, exposant plus grand, plus petit, plus petit, plus grand ?
Elève 1	Là c'est le plus petit mais enfin c'est pas le principal. On va faire avec un exemple donc…24…s'il était égal à, j'sais pas…euh… 2 exposant 1, non, bref on s'en fout, si on fait 24 sur 2.
Elève	Déjà c'est faux à partir de cette ligne !
	Oui mais bon, ça peut pas être vrai… Donc si c'était possible imagine que ça ça fasse vraiment 24, si tu divises 24 par 2, là ça t'enlèves un exposant là mais t'as toujours le 2, t'as toujours 3 fois 2 exposant 2, alors que là si tu divises par 2 il reste plus que 3 exposant 2 et donc les nombres premiers qui sont dans la décomposition c'est pas les mêmes. Avant il dit que il est d'abord manifeste que dans ce second système de facteurs il ne peut entrer d'autres nombres premiers que a, b, c etc. Tu sais il le démontre au début qu'il peut y avoir, il peut y avoir que les mêmes nombres premiers donc ça se fait au niveau de l'exposant, que même au niveau de l'exposant ça marche pas parce que tu retombes toujours sur un même nombre qui se décomposerait en produits de facteurs premiers où les nombres premiers sont pas les mêmes.
Elève	Donc sa démonstration c'est un contre exemple
Elève 1	Donc ça marche pas, voilà faut montrer que c'est pas possible, que c'est absurde.

Extrait 1.9

Cet extrait a permis d'illustrer la maladresse dans le recours à un exemple et la confusion qui est faite entre raisonnement par l'absurde et contre-exemple. Nous retrouvons (Battie, 2007) les difficultés rencontrées par certains élèves dans la mise en oeuvre de raisonnements hypothético-déductifs.

5. CONCLUSION DU COMPTE RENDU

En guise de conclusion de notre court exposé de synthèse, nous avons zoomer quelques instants sur la transition lycée-université en précisant que dans nos travaux (contribution acceptée pour *the ICMI Study 19 "Proof and proving in mathematics education"*), nous observons un transfert de l'autonomie dévolue aux élèves en termes de dimensions organisatrice et opératoire.

Les échanges qui ont eu lieu au cours de l'atelier nous amènent à mentionner des éléments de réflexion qui feront l'objet d'une communication que nous tiendrons en avril 2009 dans le cadre du colloque Espace Mathématique Francophone qui aura lieu à Dakar (*groupe de travail n°4 « Dimensions linguistique, historique et culturelle dans l'enseignement des mathématiques »).* Nous identifions deux pistes méthodologiques à la fois distinctes et susceptibles de s'articuler pour penser la dimension historique dans l'enseignement des mathématiques : l'intégration d'une dimension historique dans la classe d'une part, et l'exploitation de l'histoire des mathématiques pour concevoir des activités (au sens le plus large) pour la classe. La distinction entre ces deux pistes méthodologiques réside dans la différence de statut de l'histoire des mathématiques : dans le premier cas, l'histoire des mathématiques est avant tout objet d'étude alors que dans le deuxième elle joue le rôle d'outil didactique. Avec l'exploitation de textes historiques en classe de mathématiques, ces deux pistes se rencontrent : l'histoire des mathématiques est à la fois objet d'étude via l'étude de textes historiques et **outil didactique via l'exploitation du décalage culturel en jeu.** Ce décalage culturel permet entre autres de mettre à jour ce qui ne va pas de soi mathématiquement pour les élèves et peut ainsi aider à soulever des malentendus entre les élèves et l'enseignant. De plus, le décalage culturel en jeu dans la lecture de textes historiques favorise selon nous l'émergence non artificielle de la question de rigueur au sein de la classe. Et, selon nous, ce niveau d'exigence doit être intimement lié à l'identification des ressorts de la preuve en jeu, identification aidée par une analyse en termes de dimensions organisatrice et opératoire.

6. BIBLIOGRAPHIE

Battie, V. (2009). Le théorème fondamental de l'arithmétique: une approche historique et didactique, *Proceedings of the 5th International Colloquium on the didactics of mathematics*, University of Crete, Greece. *A paraître.*

Battie, V. (2007). Exploitation d'un outil épistémologique pour l'analyse des raisonnements d'élèves confrontés à la résolution de problèmes arithmétiques, *Recherches en didactique des mathématiques*, 27(1), pp. 9-44.

Bühler, M., Michel-Pajus, A. (2007). Sur différents types de démonstrations rencontrées spécifiquement en arithmétique, *Mnémosyne*, 19, pp. 19-60. Paris: IREM-Université Paris 7.

Campbell, S. R., Zazkis, R. (eds.) (2002). *Learning and teaching number theory: Research in cognition and instruction*, Westport, CT : Ablex Publishing.

Euclide (1994) *Les Eléments*, Volume 2, Traduit et commenté par Bernard Vitrac, Paris: PUF Coll. Bibliothèque d'histoire des sciences.

Gauss, Ch.-Fr. (1953). *Recherches arithmétiques*, Traduites par Poullet-Delisle, Paris: Librairie scientifique et technique A. Blanchard.

Goldstein, C. (1992). On a Seventeenth-Century Version of the Fundamental Theorem of Arithmetic, *Historia Mathematica*, 19, pp. 177-187.

Henry, M. (2001). Le théorème de Gauss dans les Eléments d'Euclide ?!, *Bulletin de l'APMEP* n°433.

Samuel, P. (1967). Sur l'organisation d'un cours d'arithmétique, *Bulletin de l'APMEP* n°253.

Document n°1 distribué aux groupes d'élèves

7. ANNEXES

Voici une traduction de la proposition 31 (énoncé + preuve) du Livre VII des *Eléments*[4] d'Euclide (mathématicien grec IIIème siècle avant J.-C.).

Côté vocabulaire :

- « *nombre composé* » : entier naturel qui n'est pas premier.
- *« un nombre A est mesuré par un nombre B »* ou encore *« B mesure A »* : A est divisible par B ou encore B divise A.

31

Tout nombre composé est mesuré par un certain nombre premier.

A ——————————

B ———————————

C ————————

Soit un nombre composé A. Je dis que A est mesuré par un certain nombre premier.

En effet, puisque A est composé, un certain nombre le mesurera. Qu'il le mesure et que ce soit B. Et si B est premier, ce qui était prescrit aura été fait. S'il est composé, un certain nombre le mesurera. Qu'il le mesure et que ce soit C. Et puisque C mesure B et que B mesure A, le [nombre] C mesure donc aussi A. Et, d'une part si C est premier, ce qui était prescrit aura été fait, d'autre part s'il est composé, un certain nombre le mesurera. Alors l'investigation étant poursuivie de cette façon, un certain nombre premier sera trouvé qui mesurera [A]. Car s'il ne s'en trouvait pas, des nombres en quantité illimitée mesureraient le nombre A, dont chacun serait plus petit que le précédent ; ce qui est impossible dans les nombres. Donc un certain nombre premier sera trouvé qui mesurera le [nombre] précédent et qui mesurera aussi A.

Donc tout nombre composé est mesuré par un certain nombre premier. Ce qu'il fallait démontrer.

CONSIGNES POUR CHAQUE GROUPE D'ELEVES :

1. Ecrire la preuve d'Euclide avec votre langage mathématique.
2. En utilisant la proposition 31 d'Euclide, démontrer que **tout entier naturel strictement plus grand que 1 peut s'écrire comme produit de nombres premiers** (résultat qui constitue une partie du théorème fondamental de l'arithmétique).

[4] *Source* : Euclide *Les Eléments* Volume 2 Traduit et commenté par Bernard Vitrac. Paris (1994) : PUF Coll. Bibliothèque d'histoire des sciences.

Document n°2 distribué aux groupes d'élèves

Voici un extrait des *Recherches Arithmétiques*[5] (1801) de Gauss (mathématicien allemand né en 1777 et mort en 1855) :

> 14. *Si aucun des deux nombres* a *et* b *n'est divisible par un nombre premier* p, *le produit* ab *ne le sera pas non plus.*
> […]
> 15. *Si aucun des nombres* a, b, c, d, *etc. n'est divisible par le nombre premier* p, *le produit* abcd, *etc. ne le sera pas non plus.*
> Suivant l'article précédent, *ab* n'est pas divisible par *p* ; donc il en est de même de *abc*, et ainsi de suite.
> 16. THEOREME. *Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.*
> Il est évident par les élémens, que l'on peut toujours décomposer un nombre quelconque en facteurs premiers ; mais on suppose à tort tacitement que cette décomposition ne soit possible que d'une manière. Imaginons qu'un nombre ***composé…….*** $A=a^{\alpha}b^{\beta}c^{\gamma}$ etc., *a*, *b*, *c*, etc. étant des nombres premiers inégaux, soit encore décomposable d'une autre manière en facteurs premiers. Il est d'abord manifeste que dans ce second système de facteurs il ne peut entrer d'autres nombres premiers que *a*, *b*, *c*, etc., puisque quelqu'autre que ce fût ne pourrait diviser *A*, qui est composé des premiers. De même aucun des nombres premiers *a*, *b*, *c*, etc. ne peut y manquer, car sans cela il ne diviserait pas *A* (n°15) ; la différence ne peut donc porter que sur les exposans. Or soit un nombre premier *p*, qui ait dans l'un des systèmes l'exposant *m*, et dans l'autre l'exposant *n*, *m* étant $> n$: divisons de part et d'autre par p^n, *p* restera dans l'un affecté de l'exposant $m - n$, et disparaîtra de l'autre, donc pourrait se décomposer de deux manières, dans l'une desquelles *p* n'entrerait pas, tandis qu'il resterait dans l'autre, ce qui est contre ce que nous avons démontré.

CONSIGNE POUR CHAQUE GROUPE D'ELEVES :

1. Lire le résultat n°14 : reconnaissez-vous un résultat déjà rencontré en cours ?
2. Nous avons démontré dans la 1ère partie de notre étude que tout entier strictement plus grand que 1 admet une décomposition en produit de nombres premiers. <u>En vous inspirant de la preuve de Gauss du théorème n°16</u>, démontrer qu'une telle décomposition est **unique**.

[5] *Source* : Gauss, Ch.-Fr. (1953) *Recherches arithmétiques* Traduites par Poullet-Delisle. Paris : Librairie scientifique et technique A.Blanchard Ce texte est aussi accessible sur http://gallica.bnf.fr (bibliothèque numérique de la Bibliothèque Nationale de France).

Productions écrites finales des groupes 1 et 2

Production écrite finale du groupe 1

1) Soit A ∈ N, A non premier. Il existe un entier naturel premier B tel que B | A.
Si B n'est pas premier alors un autre nombre C existe tel que C | B et comme B | A alors C | A. Si C est premier, alors A est divisible par un nombre premier et si C n'est pas premier, alors il existe encore un nombre qui divise C et ainsi de suite.
Donc tout nombre non premier est divisible par un nombre premier.
Gauss
On suppose que A ∈ N est décomposable en 2 produits différents de facteurs premiers.

- Un nombre premier ne peut pas être dans un système sans être dans l'autre : si a | A dans un système alors a | A dans l'autre etc.
- La différence ne peut donc porter que sur les exposants : on aurait $A = a^{\alpha} \times b^{\beta} \times c^{\gamma} ...$

Et $A = a^{\alpha'} \times b^{\beta'} \times c^{\gamma'} ...$ ($\alpha' < \alpha$)

Or $\frac{A}{a^{\alpha'}} = a^{\alpha-\alpha'} \times b^{\beta} \times c^{\gamma}$

et $\frac{A}{a^{\alpha'}} = b^{\beta} \times c^{\gamma}$

mais on ne peut pas avoir des nombres premiers différents comme démontré précédemment, donc la proposition est impossible.

Production écrite finale du groupe 2

I)

1) Si B | A et si C | B on obtient C | A
2) On a BA deux possibilités :
   - Soit B un nombre premier

   ⇒ la démonstration est faite
   - On a un nombre C qui divise B et on retrouve nos deux possibilités pour C.

II) Soit A un nombre quelconque :

- Si A est premier, il est divisible par 1 et lui-même.
- Si A est composé, on sait qu'il possède au moins un diviseur premier. Soit k ce diviseur premier.
  On a k | A Soit B le dividende de cette division
  Donc A=kB. k∈ N* et k≥2.
  B<A.
  - Si B est égal à 1, on a B=1. A=k. On retrouve la première hypothèse.
  - Si B est premier, on a A le produit de 2 nombres premiers.
  - Si B est composé, alors il possède au moins un diviseur premier et on reprend les étapes précédentes pour C.

Conclusion : tout nombre > 1 est le produit de nombre premier

Soit A un nombre composé.
Supposons qu'il existe au moins 2 décompositions de A : A1 et A2.
A1=A2 et A1 et A2 sont divisible par les mêmes nombres premiers a ; b ; c…

$A_1 = a^{\alpha} \times b^{\beta} \times ... \times p^{n}$

$A_2 = a^{\alpha} \times b^{\beta} \times ... \times p^{m}$ avec m>n

$\frac{A_1}{p^n} = a^{\alpha} \times b^{\beta} \times ...$

$\frac{A_2}{p^n} = a^{\alpha} \times b^{\beta} \times ... \times p^{m-n}$ $\Rightarrow \frac{A_1}{p^n} \neq \frac{A_2}{p^n} \Leftrightarrow A_1 \neq A_2$