VARIATIONS EUCLIDIENNES [1]

Norbert VERDIER [2], Olivier BORDELLES,
Bernard SCHOTT & Jean-Jacques SEITZ

L'algorithme d'Euclide est un des plus anciens algorithmes de calcul. Il permet de calculer le «Plus Grand Commun Diviseur» (PGCD) de deux nombres entiers. Sa simplicité (des divisions successives), son efficacité et la diversité de ses applications le caractérisent. Nous commençons ici par nous focaliser sur le réseau d'articles dus à des auteurs de différents profils publiés dans la presse mathématique, au milieu du XIXème siècle. Ces considérations historiques sont suivies de variations pédagogiques ayant pour objectif de mettre à la portée de nos élèves d'aujourd'hui – lycéens ou étudiants – deux types d'applications. La première est ce que nous nommons aujourd'hui le théorème de Lamé, un théorème prisé par les informaticiens. Il a pour finalité l'estimation du temps de calcul de cet algorithme et affirme que : « Le nombre de divisions à effectuer, pour trouver le plus grand commun diviseur entre deux entiers A, et B < A, est toujours moindre que cinq fois le nombre des chiffres de B ». La deuxième application est un théorème d'arithmétique de Serret, affirmant que tout nombre entier congru à un modulo quatre est somme de deux carrés. Il est obtenu ici par une relecture pertinente et moderne de l'algorithme d'Euclide due au mathématicien norvégien Axel Thue (1863-1922), au début du vingtième siècle. Ces deux applications sont mises en scène en présentant des textes testés avec des élèves de différents niveaux, par différents biais.

A – LES PRE-REQUIS MATHEMATIQUES

a) *Théorème de la division euclidienne*

En arithmétique, le théorème de la division euclidienne est essentiel. Ce théorème affir-

1 Ce texte a été considérablement enrichi par les remarques constructives et structurelles des rapporteurs. Nous tenons à les remercier ici pour leur collaboration indirecte.
2 IUT Cachan & GHDSO (Université Paris-Sud).

me que l'on peut toujours diviser deux nombres entiers naturels entre eux. Dit plus précisément, si on considère deux entiers naturels a et b, il existe un nombre quotient q et un reste r tel que : $a = bq + r$ avec $0 \leq r < b$.

Par exemple, si on divise 981 par 41 on trouve, en effectuant la division qu'on a apprise à l'école primaire, que le quotient vaut 23 et le reste 38. Quand on trouve un reste nul on dit que « b divise a » ou que « a est divisible par b » ou encore que « b est un diviseur de a ».

b) *L'algorithme d'Euclide*

Le théorème de la division euclidienne permet de construire une méthode de calcul — un algorithme —, permettant de calculer le PGCD (Plus Grand Commun Diviseur) de deux nombres. Pour des cas élémentaires, la valeur du PGCD est triviale. Par exemple, le PGCD de 21 et 15 vaut 3. En revanche que dire du PGCD de 1597 et 987 ? L'algorithme d'Euclide permet de calculer le PGCD de deux nombres a et b (entiers naturels non nuls) par une succession de divisions : on divise successivement a par b ; puis b par le reste trouvé ; puis le premier reste par le deuxième reste ; le deuxième par le troisième ; etc. jusqu'à ce qu'on trouve un reste nul. Le dernier reste non nul est le PGCD de a et b. En notant, les restes successifs $r_1, r_2, \ldots$ on peut récapituler l'ensemble des divisions sous forme du tableau suivant :

a	r_1	r_3	…	…	0
b	r_1	r_4	…	r_k	FIN

et conclure que le PGCD de a et b vaut r_k. Notons que l'algorithme est décrit dans les *Éléments* d'Euclide avec d'autres mots ; en particulier, il est fondé sur des soustractions successives (ce qui n'est qu'une autre manière de réaliser des divisions !).

Par exemple si $a = r_0 = 21$ et $b = r_1 = 15$, nous trouvons que $r_3 = 6$, $r_4 = 3$ et $r_5 = 0$; donc PGCD (21, 15) = 3.

Si on trouve pour PGCD le nombre 1, on dit que les nombres « a et b sont premiers entre eux ».

L'algorithme d'Euclide offre d'emblée des applications immédiates : il permet de « développer un nombre en fractions continues » : la première étape (la division de a par b) permet d'écrire :

$$\frac{a}{b} = q_1 + \frac{r_1}{b}$$

mais, d'après la seconde étape : $b = q_2 r_1 + r_2$ d'où

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}$$

et ainsi de suite. En généralisant, il vient :

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}}}$$

L'algorithme d'Euclide permet surtout de démontrer un autre théorème capital : le théorème (encore faussement attribué aujourd'hui à Bézout) car, un siècle avant Bézout, Bachet de Méziriac (1581-1638), dès

la deuxième édition de ses *Problèmes plaisants et délectables*, questionnait: « Deux nombres premiers étant donnés, trouver le moindre multiple de chacun d'iceux, surpassant de l'unité un multiple de l'autre. »

Dit autrement, il s'agit, avec le vocabulaire d'aujourd'hui, de résoudre (en nombres entiers) l'équation : $an = bm + 1$, un forme de l'identité dite aujourd'hui « de Bézout ».

B – PREMIERE VARIATION AUTOUR D'UN THEOREME «DE LAME»

Comme toujours en mathématique, dès qu'on dispose d'un algorithme, on s'intéresse à son efficacité. Comment « mesurer » son efficacité, son « temps de calcul » ? C'est l'objet d'une note, chère aux informaticiens d'aujourd'hui, publiée en 1844 par Gabriel Lamé (1795-1870) : « Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers ». [Lamé, 1844].

a) *Le théorème « de Lamé »*

Quand il publie sa note en 1844 aux *Comptes rendus hebdomadaires de l'Académie des sciences*, Lamé vient juste d'être nommé académicien l'année précédente. Il commence ainsi son mémoire :

> « Dans les traités d'Arithmétique, on se contente de dire que le nombre des divisions à effectuer, dans la recherche du plus grand commun diviseur entre deux entiers, ne pourra pas surpasser la moitié du plus petit. Cette limite, qui peut être dépassée si les nombres sont petits, s'éloigne outre mesure quand ils ont plusieurs chiffres. » [Lamé, 1844]

avant d'établir « son » théorème : « Le nombre de divisions à effectuer, pour trouver le plus grand commun diviseur entre deux entiers A, et B < A, est toujours moindre que cinq fois le nombre des chiffres de B ». [*Ibid*.]

Sa démonstration repose judicieusement sur l'emploi des nombres dit aujourd'hui de Fibonacci que Lamé définit ainsi :

> « Si, commençant par 1 et 2, on compose une suite de nombres entiers, tels que chacun d'eux soit égal à la somme des deux nombres qui le précèdent, on obtient la série suivante :
> (1) 1, 2, 3, 5, 8 ; 13 , 21, 34, 55, 89 ; 144, 233, 377, 610, 987 ; 1597 … » [*Ibid*.]

Il termine son mémoire par un exemple marquant la force de son théorème :

> « Soient pris, pour exemple, les deux nombres 1597 et 987 [16e et 15e terme de la série (1)]. La recherche de leur plus grand commun diviseur se composera de 14 divisions. Le limite assignée par le théorème actuel est 15. La limite adoptée dans les traités d'Arithmétique serait 493.» [*Ibid*.]

Le théorème de Lamé est le « premier » théorème s'intéressant à l'efficacité de l'algorithme d'Euclide. Plus tard, Edouard Lucas (1842-1891) montre le caractère optimal du théorème de Lamé. Si l'histoire ne retient que le nom de Lamé, force est de constater que le tamis du temps a fait oublier d'autres « contributeurs » qui, au milieu du XIXème siècle, ont apporté chacun à leur mesure leur pierre à l'édifice.

b) *Lamé et les autres*

N'attribuer qu'à Lamé le théorème dit de Lamé serait nier la profusion d'articles

qu'il a suscité dans la première moitié du XIXème siècle. Lamé impose « son » théorème par sa surface institutionnelle (il vient d'être élu membre de l'Académie des Sciences en 1843) et sa possibilité d'accès aux *Comptes Rendus hebdomadaires de l'Académie des sciences* — ce « Tribunal de la Science » selon l'expression de Hugues Chabot[3].

Lamé ne cite pas dans son travail ses devanciers[4] et se contente de faire référence au terme générique : « traités d'arithmétique » comme nous l'avons vu lorsque nous avons cité précédemment le début de son article.

Jeffrey Shallit s'est intéressé dans son article intitulé « Origins of the Analysis of the Euclidean Algorithm » [Shallit, 1994][5] aux premiers travaux autour du « temps de calcul » de l'algorithme d'Euclide. Cet article mérite quelques compléments. Nous nous contenterons ici de dégager un corpus de textes traitant de ce sujet. Il est synthétisé dans le tableau[6] ci-contre.

L'étude du détail des textes montre le rôle joué par les *Nouvelles Annales de Mathématiques* — lancées en 1842 —; elles sont un nouveau moyen d'expression pour des auteurs, pour la plupart inconnus ou méconnus du monde scientifique académique, qui sans ce biais devaient souvent se contenter d'une citation (sans rapport) à l'Académie des sciences.

Travaux sur l'algorithme d'Euclide publiés entre 1836 et 1851

Nom de l'auteur	Année public.	Nature support	Référence
Léger	1836	JMPA	[Léger, 1836]
Léger	1837	CMP	[Léger, 1837]
Finck	1841	*Traité élé. d'arithm.*	[Finck, 1841]
Binet	1841	JMPA	[Binet, 1841]
Finck	1842	NA	[Finck, 1842]
Lamé	**1844**	**CRAS**	**[Lamé, 1844]**
Binet	1844	CRAS	[Binet, 1844]
Gros	1844	CRAS	[Gros, 1844]
Finck	1845	NA	[Finck, 1845]
Lionnet	1845	NA	[Lionnet, 1845]
Nievengloski	1845	NA	[Nievengloski, 1845]
Dupré	1846	JMPA	[Dupré, 1846]
Dupré	1848	JMPA	[Dupré, 1848]
Nievengloski	1849	NA	[Nievengloski, 1849]
Lionnet	1851	NA	[Lionnet, 1851]

c) *La proposition pédagogique*

Expérimenter, prendre des exemples, conjecturer, mettre en œuvre des outils de démonstration, critiquer la pertinence des résultats, font partie des savoir-faire qui seront mis en œuvre lors de l'épreuve pratique de mathématiques du bac S, dès le mois de juin 2008 et à titre expérimental dans certaines académies. Il s'agit d'évaluer la capacité à étudier un problème posé, en utilisant les

3 Hugues Chabot, «Le tribunal de la science. Les rapports négatifs à l'Académie des sciences comme illustrations d'un scientifiquement (in)correct (1795-1835)», in *Annales historiques de la Révolution française*, Numéro 320, [En ligne], mis en ligne le : 23 janvier 2006. URL : http://ahrf.revues.org/document161.html.

4 La plupart des traités (dès le XIXe) ne retiennent d'ailleurs que la contribution de Lamé. Soulignons toutefois que Lucas en fin de siècle (Cf. Lucas, Edouard, *Théorie des nombres*, 1891, Gauthier-Villars, 333-339.) fait référence aux travaux antérieurs de Finck et Léger.

5 Cet article a été historiquement complété par Peter Schreiber dans son article «A Supplement to J. Shallit's Paper «Origins of the Analysis of the Euclidean Algorithm»», *Historia Mathematica,* 22 (1995), 422-424. Peter Schreiber mentionne les contributions de Simon Jacob au XVI ème siècle en Allemagne.

6 JMPA désigne le *Journal de Mathématiques Pures et Appliquées* c'est-à-dire le *Journal de Liouville*; CMP désigne la *Correspondance Mathématique et Physique* c'est-à-dire la *Correspondance de Quételet*; CRAS désigne les *Comptes Rendus Hebdomadaires de l'Académie des Sciences* et NA désigne les *Nouvelles Annales de Mathématiques*.

TICE de manière significative. Dans l'esprit actuel de cette épreuve pratique de mathématiques en classe de Terminale S, mais de longueur inadaptée, voici une illustration du théorème de Lamé. Il s'agira de conjecturer puis de démontrer un résultat donnant une majoration du nombre d'étapes nécessaires à l'algorithme d'Euclide. **[Cf. Annexe A]**

Une première partie est consacrée à la suite de Fibonacci. Ensuite, l'algorithme d'Euclide est mis en place. Nous nous intéressons au coût de ce processus, c'est-à-dire aux nombres de pas nécessaires à l'aboutissement du procédé. Enfin, après observations, une démonstration du théorème de Lamé est proposée. Les prérequis mathématiques sont :

— Mettre en place le principe de récurrence forte.

— Connaître quelques propriétés de la fonction ln .

— Maîtriser quelques outils d'arithmétique : divisibilité dans **Z**, pgcd, algorithme d'Euclide, …

L'activité qui suit est la synthèse de plusieurs remarques et interrogations de la part d'élèves d'une classe de Terminale S, au moment où sont étudiées les suites. Deux réflexions en particulier ont émergé d'une séance :

- Tout d'abord le raisonnement par récurrence a été critiqué et jugé par certains élèves comme « répétitif ». L'idée de proposer le principe de récurrence forte est donc venue.
- Certains élèves ont essayé d'imaginer le comportement de suites convergentes d'entiers naturels. Comme se rapprocher de la limite en restant dans l'ensemble des entiers ? J'ai proposé alors de construire et d'observer une suite d'entiers naturels, décroissante. Dans un premier temps, les élèves ne sont pas parvenus à exhiber une telle suite.

L'activité a été proposée sous la forme d'un « Devoir Maison », qu'une partie des élèves a traité avec succès, les autres préférant un énoncé plus classique.

Le texte a également été testé avec des étudiants de l'IUT de Cachan lors de l'année 2007–2008 dans le cadre d'un «projet sciences»[7]. Une équipe de quatre étudiants souhaitant poursuivre leurs études dans une école d'ingénieurs à dominante informatique a eu six semaines pour traiter la partie théorique (la démonstration du théorème « de Lamé » présenté ici et pour concevoir un programme informatique à l'aide d'un logiciel de calcul formel *Mathematica* ou *Maple*). Nous présentons en annexe **[Cf. Annexe B]** une résolution avec *Maple*. Une autre équipe de deux étudiants (de niveau mathématique plus faible) a seulement travaillé sur les aspects informatiques en admettant la partie théorique sous-jacente.

d) *Pour aller plus loin*

Cette « mise en pratique » d'un théorème concernant l'algorithme d'Euclide peut être éten-

7 Un «projet science» désigne à l'IUT de Cachan un projet effectué en autonomie par un binôme (c'est un peu l'équivalent des TPE au lycée). Chaque binôme doit traiter un sujet relevant des sciences. Certains sujets sont choisis, d'autres sont «suggérés». Ainsi, nous orientons les étudiants désireux de poursuivre leurs études vers des écoles d'ingénieurs sélectives (Supelec, INSA, ENSI, etc.) vers des sujets traditionnellement plus difficiles L'an dernier, au colloque Geii de Marseille, nous avons dressé un bilan sur 10 ans de projet sciences à l'IUT de Cachan. Cf. Norbert Verdier, «Les projets sciences à l'IUT de Cachan (Geii1)», Colloque Geii, Marseille, 30 mai-1er juin 2007.

due dans diverses directions. Dans le réseau d'articles constituant le corpus d'étude que nous avons mis en valeur dans l'étude préliminaire, nous envisageons « d'explorer pédagogiquement » les contributions de Dupré.

Entré en 1826, à l'École normale, il enseigne au Collège Royal de l'Arc à Dôle puis est envoyé au lycée de Rennes où il y fait toute sa carrière[8]. Au moment où il soumet une note à l'Académie des sciences, il est déjà depuis longtemps professeur de lycée et souhaite sans doute donner une seconde vie à sa carrière. Sa note, présentée à l'Académie, est reçue avec intérêt mais n'est pas publiée dans les *Comptes rendus*, en revanche elle est publiée dans le *Journal de Liouville* en 1846 [Dupré, 1846]. Il cite les travaux de Lamé et Binet et rédige — pour reprendre ses mots — « ce qu ['il a] à dire sur le sujet » [*Ibid*., 41]. Son additif de 1848 [Dupré, 1848] est une extension de son travail de 1846. Désormais, Dupré est devenu professeur de mathématiques appliquées à la Faculté des sciences de Rennes.

Il s'intéresse dans son article au « nombre de divisions à effectuer pour trouver le plus grand commun diviseur entre deux nombres complexes de la forme $a+b\sqrt{-1}$, où a et b sont entiers » [Dupré, 1848]. Autrement dit, il s'intéresse au PGCD de deux entiers dits de Gauss. Sans analyser tout son article, Dupré commence par définir en quoi consiste le théorème de la division euclidienne pour deux entiers de Gauss.

Prenons un exemple (qui n'est pas dans l'article de Dupré) mais qui est développé à partir des considérations générales de Dupré. Soit $a = -36 + 242\,i$ et soit $b = 50 + 50\,i$. En effectuant le quotient a par b, nous obtenons :

$$a/b = 103/50 + 139/50\,i$$

En extrayant « les entiers contenus » dans les parties réelles et imaginaires, il vient que :

$$103/50 = (100+3)/50 = 2 + 3/50$$

et $$139/50 = (150-11)/50 = 3 - 11/50$$

Ainsi : $$\begin{aligned} a &= (2 + 3i)b + (3/50 - 11/50i)b \\ &= (2 + 3i)\,b + 14 - 8\,i. \end{aligned}$$

Le reste de cette division de a par b est $14 - 8\,i$; par construction, il vérifie le fait que son module (ici $2\sqrt{65}$) est strictement inférieur à celui de b (qui vaut ici $50\sqrt{2}$). Le théorème de la division euclidienne est donc conservé.

Dupré oriente ainsi son travail de généralisation vers ce que nous nommons aujourd'hui les anneaux euclidiens c'est-à-dire des ensembles ayant une structure algébrique d'anneau dans lequel le théorème de la division euclidienne est possible. L'anneau des entiers naturels et l'anneau des entiers de Gauss sont les prototypes d'anneau euclidien; l'anneau des polynômes à coefficients dans un corps commutatif est un autre exemple[9]. Les textes de Dupré peuvent être (en totalité ou en partie) explorés avec des étudiants de différents niveaux **[Cf. Annexe C].**

8 Plusieurs notes nécrologiques ont permis de reconstituer la carrière de Dupré: Cf. *L'Année scientifique et industrielle*, 1870, pp. 587-588; S. Sirodot, «Athanase Louis Victor Dupré», *Université de France, Académie de Rennes*, 1869, 52-57 et Louis Joubin, *Histoire de la Faculté des sciences de Rennes*, 1900, 153-155.

9 Il est d'ailleurs intéressant d'explorer à cette occasion le monde de la non - commutativité : que devient l'algorithme d'Euclide pour le calcul du PGCD de deux polynômes qui sont dans un anneau non commutatif? Cette question est l'objet d'une très intéressante discussion sur le forum de Les Mathématiques.net (Cf. http://les-mathematiques.u-strasbg.fr/phorum5/read.php?3,407019,407106#msg-407106.).

D'autres exemples d'applications possibles en classe (plutôt à l'Université mais certains textes sont utilisables en lycée) figurent dans le chapitre « The Greatest Common Divisor » du livre de Eric Bach & Jeffrey Shallit intitulé *Algorithmic number theory* [Bach & Shallit, 1996, 67-100].

C – DEUXIEME VARIATION AUTOUR D'UN THEOREME DE SERRET

a) *Un théorème dans son contexte*

Joseph-Alfred Serret, en 1844, se livre à la démonstration d'une propriété arithmétique « connue » : « *Tout nombre premier $4k + 1$ est la somme de deux carrés* »[10] [Serret, 1848]. En cherchant à démontrer cette décomposition particulière en somme de carrés, il explique qu'il a rencontré des propositions « qui lui semblent dignes d'être signalées » [*Ibid*.]. Son travail est essentiellement fondé sur l'emploi des fractions continues. Nous présentons ici sous forme d'un problème proposé au niveau des classes préparatoires sous forme d'un « devoir maison » la résolution du résultat. Nous nous appuyons sur une autre approche déduite de l'algorithme de Thue[11] qui est une autre façon d'explorer l'algorithme d'Euclide.

Pour faire utiliser à nos élèves le théorème de Serret, nous avons découpé l'étude en trois parties. La première partie consiste à démontrer « le lemme de Thue » qui constitue un outil classique de la théorie élémentaire des nombres. La seconde partie a pour objectif la démonstration du « théorème des deux carrés ». Ce théorème, qui aurait été conjecturé par Fermat un certain 25 décembre 1640, est également connu sous le nom de « Théorème de Nöel ». Il stipule qu'un nombre premier p s'écrit comme somme de deux carrés si et seulement si : $p = 2$ ou $p \equiv 1 \pmod 4$. La troisième partie s'appuie sur le théorème de Serret pour construire explicitement un couple (u, v) d'entiers tels que : $p = u^2 + v^2$. Par la suite, on se restreindra au cas où p est un entier impair, puisque le cas $p = 2$ est trivial (par la décomposition en somme de deux carrés: $2 = 1^2 + 1^2$). D'autre part, nous désignerons par $[t]$ la partie entière de t et par $\mathrm{mod}(n, m)$ le reste de la division de n par m.

b) *Le texte soumis aux élèves* **[Annexe D]**

c) *Expériences pédagogiques*

Ce texte a également été proposé partiellement à l'IUT de Cachan à un groupe d'étudiants chinois lors de l'année universitaire 2007-2008[12]. Nous avons testé ce problème selon le cheminement suivant. Ces étudiants, durant les 15 semaines de préparation, suivent, en plus des cours de français, un enseignement de mathématiques qui n'obéit pas *stricto sensu* à un programme mais qui a pour but de les familiariser au « français technique ». Nous avons consacré cette année une séance à préparer aux savoirs mis en jeu dans la première partie du problème (vocabulaire des congruences, notion de démonstration par l'absurde, etc.). En fin de séance, nous avons

10 Cette phrase est composée en italiques dans le corps du texte.

11 Pour avoir des informations biographiques sur Thue, nous renvoyons à la source indiquée en sitographie. Pour des informations sur la pratique mathématique de Thue, nous renvoyons à l'article de Maurice Margenstern, «L'école constructive de Markov», *Revue d'histoire des mathématiques* **1**, fascicule 2 (1995), 271-305.

12 Depuis 2006-2007, une vingtaine d'étudiants sélectionnés parmi quatre cents environ vient suivre quelques mois d'enseignement de français (essentiellement) à l'IUT de Cachan avant de poursuivre l'année suivante dans des formations IUT de l'Université de Paris Sud (Cachan, Orsay ou Sceaux).

donné en travail préparatoire la première partie. Les deux séances suivantes ont été consacrées à la correction. Des étudiants ont proposé des éléments de correction. Des critiques ont été formulées. Nous avons adopté la même structure pour les deux autres parties. Une synthèse écrite globale a été donnée à partir des éléments de correction figurant dans l'ouvrage de Olivier Bordellès [Bordellès, 2006, 37, 88, 168-169, 185]. Nous avons donc consacré 9 heures à ce problème dans un contexte « très spécifique » [13]. Ce problème ainsi posé nous paraît bien approprié pour des étudiants visant des concours de « très » grandes écoles d'ingénieurs. Aucun d'entre nous n'officiant en classes préparatoires, nous serions heureux si des enseignants de ces classes pouvaient tester ce problème avec leurs élèves.

Pour conclure

Cet article est le fruit d'un groupe d'étude de la presse scientifique et technique au XIXème siècle [14]. Ce groupe a été fondé et est animé par Christian Gérini et Norbert Verdier au sein du Groupe d'Histoire et de la Diffusion des Sciences d'Orsay (GHDSO — Université Paris-Sud). Un de nos objectifs est de confronter (sur des thématiques précises ici des thématiques empruntées à l'arithmétique) des textes d'hier à des enseignements d'aujourd'hui. Notre ambition est de présenter des approches, des variations possibles s'appuyant sur des documents réels ou numérisés, désormais à portée de main de chacun grâce aux intenses programmes de numérisation (publiques, comme Gallica, Numdam, etc., ou privées, comme google.books) et de référencements récents et à venir.

Cet article a été constitué de variations arithmétiques. Des chemins ont été pris, d'autres ont été suggérés, de nombreux restent à prendre. En ce sens, notre texte s'inscrit dans la lignée de deux précédents article déjà publiés dans *Repères* [Gérini & Verdier, 2007] & [Gérini, 2008]. D'autres études ont été publiées ou sont à venir par divers canaux de diffusion (articles, colloques et mises en ligne). Nous pensons en particulier à un travail autour d'une notion de géométrie différentielle (le repère dit de Serret-Frenet). Il a fait l'objet d'une intervention au colloque CNRIUT [15] de Lyon (2008) au cours de laquelle nous avons insisté sur les conditions de production de ce célèbre repère (en étudiant les rôles respectifs du parisien Serret et du lyonnais Frenet à une période où la césure Paris/Province prend toute sa mesure). Un autre projet, autour du calcul intégral, est en cours d'élaboration avec deux collègues du CEGEP de Rimouski (Philippe Etchecopar et Jean-Philippe Villeneuve) [16].

13 Deux étudiants (particulièrement brillants) ont réussi à faire la totalité du problème avec des indications. Ces étudiants avaient réussi en Chine l'examen d'entrée (en mathématiques) dans les universités chinoises les plus cotées à Pékin et à Shanghai. Ces deux étudiants auraient le niveau mathématique requis pour entrer dans une classe préparatoire française « assez sélective ». Les autres étudiants (de niveau plus modeste) ont éprouvé des difficultés mathématiques pour comprendre les subtilités du problème.

14 Le blog http://jst19eme.over-blog.com/ (en cours de réalisation) recense quelques pistes d'études et de réflexions menées par notre groupe.

15 Ce 14ème Colloque National de la Recherche en IUT (CNRIUT) s'est tenu les 29 et 30 mai 2008 à Lyon-Villeurbanne, IUT A, Université Claude Bernard Lyon 1, Campus de la Doua. Il s'agisait de l'exposé de Norbert Verdier, « Jean-Frédéric Frenet (1816-1900) à Lyon. Géométrie différentielle & calcul infinitésimal pour des élèves d'hier et d'aujourd'hui ».

16 Cette collaboration a déjà pris la forme de plusieurs travaux d'étudiants du CEGEP de Rimouski et de l'IUT de Cachan. Ces étudiants, sous notre direction, se sont focalisés sur l'introduction du calcul infinitésimal au Québec sous l'impulsion de l'abbé Langevin . Cf. http://www.cegep-rimouski.qc.ca/dep/maths/PageLangevin.htm. D'autres travaux sont en cours de réalisation.

Cette diversité de projets de tailles inégales et impliquant différents collègues intervenant à des niveaux variés, en France et à l'Étranger, est cimentée par une même et double unité: faire de l'histoire des mathématiques en s'appuyant sur des enseignements possibles et enseigner des mathématiques en s'appuyant sur des moments d'histoire. Dans cette double perspective, la salle de classe (de la maternelle à l'université selon l'expression consacrée) devient le laboratoire, direct ou indirect, de l'historien.

Bibliographie

Bach, Éric & Shallit, Jeffrey
1996. *Algorithmic number theory*, volume 1, Efficients algorithms, The MIT Press, 1996.

Binet, Jacques
1841. «Recherches sur la théorie des nombres entiers et sur la résolution de l'équation indéterminée du premier degré qui n'admet que des solutions entières», *Journal de Mathématiques Pures et Appliquées*, I, **6** (1841), 449-494.
1844. «Note sur le nombre des divisions à effectuer pour obtenir le plus grand diviseur commun de deux nombres entiers; suivie d'une remarque sur une classe de séries récurrentes», *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, **XIX** (1844), 937-941.

Bordellès, Olivier
2006. *Thèmes d'arithmétique avec plus de 85 exercices corrigés*, Ellipses, 2006.

Dupré, Athanase
1846. «Sur le nombre des divisions à effectuer pour obtenir le plus grand commun diviseur entre deux nombres entiers», *Journal de Mathématiques Pures et Appliquées*, I, **11** (1846), 41-64.
1848. «Sur le nombre de divisions à effectuer pour trouver le plus grand commun diviseur entre deux nombres complexes de la forme $a+b\sqrt{-1}$, où a et b sont entiers», *Journal de Mathématiques Pures et Appliquées,* I, **13** (1848), 333-343.

Gérini, Christian
2008. «Variations pédagogiques sur un article de géométrie analytique d'Haton de la Goupillière paru en 1872», *Repères*, **71** (Avril 2008), Topiques éditions, 65-80.

Gérini, Christian & Verdier, Norbert
2007. «Les *Annales de Gergonne* (1810-1832) et le *Journal de Liouville* (1836-1874) : une mine de textes numérisés à exploiter dans notre enseignement.», *Repères*, **67** (Avril 2007), Topiques éditions, 55-68,

Finck, Étienne
1841. *Traité élémentaire d'arithmétique*, Paris, Mathias, 1841.
1842. «Lettre sur une note de M. Vincent et sur les recherches du P.G.C.D. en arithmétique», *Nouvelles Annales de Mathématiques*, **1** (1842), 353-355.
1845. «Observations sur le théorème de M. Lamé, relativement au plus grand commun diviseur, et nouvelle démonstration de ce théorème», *Nouvelles Annales de Mathématiques*, **4** (1845), 71-74.

Gros [17]
1844. «Note sur la limite des divisions à effectuer pour trouver le plus grand commun diviseur entre deux nombres donnés», *Comptes rendus hebdomadaires de l'Académie des sciences*, **XIX** (1844), 1040.

Lamé, Gabriel
1844. «Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers», *Comptes rendus hebdomadaires de l'Académie des sciences*, **XIX** (1844), 867-870.

Léger, Émile
1836. «Mémoire sur les rapports et les restes des quantités incommensurables», *Journal de Mathématiques Pures et Appliquées*, I, **1**(1836), 93-99.
1837. «Note sur le partage d'une droite en moyenne et extrême, et sur un problème d'arithmétique», *Correspondance mathématique et physique*, **9** (1837), 483-485.

Lionnet, Eugène
1845. «Sur la limite du nombre des divisions à faire pour trouver le plus grand commun diviseur de deux nombres entiers», *Nouvelles Annales de Mathématiques*, **4** (1845), 617-626.
1851. «Note sur le plus grand commun diviseur», *Nouvelles Annales de Mathématiques*, **10** (1851), 85-86.

17 Nous ignorons le prénom de ce mathématicien qui selon les Catalogue of scientific papers n'est l'auteur que d'une seule note aux *Nouvelles Annales de Mathématiques* en 1860 et est co-auteur avec Eugène Prouhet des *Solutions raisonnées des exercices proposés dans le traité d'arithmétique* de M. Joseph Bertrand, chez Hachette, en 1850.

Nievengloski, G.H. [18]

1845. «Sur la limite supérieure du nombre de divisions à faire pour trouver le plus grand commun diviseur de deux nombres», *Nouvelles Annales de mathématiques*, **4** (1845), 568-573.

1849. «Note sur une abréviation dans la recherche du plus grand commun diviseur de deux nombres», *Nouvelles Annales de mathématiques*, **8** (1849), 447-448.

Serret, Joseph, Alfred

1848 «Sur un théorème relatif aux nombres entiers», *Journal de Mathématiques Pures et Appliquées*, I, **13** (1848), 12-14.

Shallit, Jeffrey

1994. «Origins of the Analysis of the Euclidean Algorithm», *Historia Mathematica*, **21,** (1994), 401-419.

Sitographie

http://www.math.u-bordeaux.fr/~lasjauni/page_fr_0.htm [Un site dédié à la mémoire de Axel Thue et présentant certains de ses apports].

18 Nous n'avons pas d'indication sur le prénom.

ANNEXES

A - Le « théorème de Lamé » soumis aux élèves

I – *La suite de Fibonacci*

On appelle suite de Fibonacci, la suite (u_n) définie par : $u_0 = u_1 = 1$; $u_{n+2} = u_{n+1} + u_n$ pour tout n entier naturel. Pour la suite, on posera : $\varphi = \frac{1+\sqrt{5}}{2}$.

1) Démontrer que $\varphi^2 = \varphi + 1$, puis que pour tout entier naturel n nul on a $\varphi^{n+1} = \varphi^n + \varphi^{n-1}$
En déduire que, pour tout entier naturel n non nul : $u_{n+1} \geq \varphi^n$.

2) A l'aide d'un tableur, calculer les vingt premiers termes de la suite de Fibonacci.

3) Dans la même feuille de calcul du tableur, faire apparaître le pgcd de deux termes consécutifs de la suite de Fibonacci.
   a) Que peut-on conjecturer pour u_n et u_{n+1} pour tout n ?
   b) Démontrer ce résultat.

4) Démontrer que pour tout entier naturel n, le reste de la division euclidienne de u_{n+2} par u_{n+1} est u_n.

II – *L'algorithme d'Euclide*

L'algorithme d'Euclide peut être mis en place sous la forme suivante : soient deux entiers distincts non nuls r_0 et r_1, avec par exemple $r_0 > r_0$. Par divisions euclidiennes successives, on a :

$r_0 = q_1 r_1 + r_2$ avec $0 < r_2 < r_1$

$r_0 = q_2 r_2 + r_3$ avec $0 < r_3 < r_2$

… …

$r_{n-2} = q_{n-1} r_{n-1} + r_n$ avec $0 < r_n < r_{n-1}$

$r_{n-1} = q_n r_n + 0$

et pgcd (r_0 , r_1) = r_n , le dernier reste non nul.

Dans ce cas, on dira que l'algorithme d'Euclide a nécessité n divisions ou n étapes.

1) Sur une feuille de calcul du tableur, construire l'algorithme d'Euclide. Calculer par exemple de cette façon le pgcd de 55 et 34. Combien d'étapes ont été mises en œuvre dans ce cas ? Le nombre d'étapes n'est a priori pas prévisible : la recherche du pgcd de 55 et 33, par exemple, sera plus courte.

2) Exécuter l'algorithme d'Euclide avec deux termes consécutifs de votre choix de la suite de Fibonacci u_{n+1} et u_n. Combien d'étapes sont nécessaires ? Démontrer ce résultat à l'aide de la question I.4.

3) Déterminer deux entiers non nuls, où le plus petit des deux s'écrit avec un seul chiffre, et tels que le nombre d'étapes dans l'algorithme d'Euclide soit exactement 5.

4) Déterminer deux entiers non nuls, où le plus petit des deux s'écrit avec deux chiffres, et tels que le nombre d'étapes dans l'algorithme d'Euclide soit exactement 10.

5) En généralisant, peut-on trouver deux entiers, où le plus petit des deux s'écrit avec k chiffres, tels que le nombre d'étapes dans l'algorithme d'Euclide soit $5k$?

III – *Un théorème de Lamé*

La dernière partie a pour but de démontrer le théorème suivant : « Le nombre de divisions euclidiennes nécessaires pour obtenir le pgcd de deux entiers naturels non nuls, en appliquant l'algorithme d'Euclide, est inférieur ou égal à 5 fois le nombre de chiffres servant à écrire le plus petit des deux nombres. »

La suite de Fibonacci est toujours notée (u_n). Considérons l'algorithme d'Euclide suivant où n, le nombre d'étapes, est un entier naturel fixé :

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && \text{avec } 0 < r_2 < r_1 \\
r_0 &= q_2 r_2 + r_3 && \text{avec } 0 < r_3 < r_2 \\
&\dots && \dots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && \text{avec } 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0\ , && \text{pgcd}\,(r_0\ , r_1) = r_n\ ,
\end{aligned}$$

1) a) Montrer que $q_n \geq 2$ et en déduire que $r_{n-1} \geq u_2$.

b) Démontrer par récurrence sur k que pour tout entier k tel que $1 \leq k \leq n$, on a $r_{n-k} \geq u_{1+k}$.

2) En déduire alors que $r_1 \geq u_n$. En vous aidant de la première partie, démontrer que $r_1 \geq \varphi^{n-1}$.

3) Vérifier que $\ln\varphi \geq \dfrac{\ln 10}{5}$ puis en déduire que $\ln r_1 \geq (n-1)\dfrac{\ln 10}{5}$.

4) En supposant que r_1 s'écrive avec k chiffres, expliquer pourquoi $r_1 < 10^k$. En déduire finalement $n \leq 5k$.

B - Un programme avec Maple pour donner le pgcd de deux nombres et le nombre de divisions effectuées

Attention : toujours écrire dans l'ordre (a,b) avec a > b

```
Ø pgcd := proc(a,b)
local u ,v, r, n,L;
u := a;
v := b;
r := 1;
n := 1;
while r>0 do
r := irem(u,v);
u := v;
v := r;
L := [u,n];
n := n+1;
end do;
return L;
end proc;
```

et dans pgcd(a,b); on affiche L= [u,n] , le premier terme u est le pgcd, et le second n est le nombre de divisions nécessaires pour obtenir ce pgcd..

Exemples :

pgcd(13,8); [1,5]
pgcd(12,6); [6,1]
pgcd(90,12); [6,2]
pgcd(1597,987); [1,15]

C - Un exercice extrait de l'article de Dupré [Dupré, 1848]

a) Soit un entier de Gauss. Ce nombre sera premier s'il n'est divisible par aucun autre nombre de même forme que lui-même, en excluant néanmoins +1, – 1, i, et – i, qui jouent dans cette théorie le même rôle que l'unité. – 36 + 242 i est-il premier ?

b) « Si [un] nombre premier divise le produit AB de deux autres nombres complexes, il divisera nécessairement l'un d'eux »

Pour suivre la discussion associée à cet exercice :

http://les-mathematiques.u-strasbg.fr/phorum5/read.php?17,416137,417068#msg-417068

D - L'algorithme de Serret soumis aux élèves

1 Partie 1 : le lemme de Thue

Le but de cette partie est la démonstration du résultat suivant :

Théorème 1 (Lemme de Thue). *Soient $a > 1$ entier et $p \geqslant 3$ premier tels que $p \nmid a$. La congruence $au \equiv v \pmod p$ a un couple solution $(u, v) \in \mathbb{Z}^2$ vérifiant :*

$$\begin{cases} 1 \leqslant |u| < \sqrt{p}, \\ 1 \leqslant |v| < \sqrt{p}. \end{cases}$$

1°. On note $E = \{0, \dots, [\sqrt{p}]\}^2$ et on définit sur E une application f, à valeurs dans $\{0, \dots, p-1\}$, par $f(u, v) = \text{reste}(au - v, p)$. Montrer que f n'est pas injective.

2°. On note (u_1, v_1) et (u_2, v_2) deux couples tels que $(u_1, v_1) \neq (u_2, v_2)$ et $f(u_1, v_1) = f(u_2, v_2)$, et on pose $u = u_1 - u_2$ et $v = v_1 - v_2$.

(a) Vérifier que $au \equiv v \pmod p$ et que $|u| < \sqrt{p}$ et $|v| < \sqrt{p}$.

(b) Montrer par l'absurde que $u \neq 0$, puis que $v \neq 0$.

2 Partie 2 : le théorème des deux carrés

1°. Soit $p \geqslant 3$ un nombre premier tel qu'il existe deux entiers a, b tels que $p = a^2 + b^2$. Montrer que $p \equiv 1 \pmod 4$.

2°. On suppose que $p \equiv 1 \pmod 4$ et on pose $x \equiv \left(\frac{p-1}{2}\right)! \pmod p$.

(a) Vérifier que $p \nmid x$ et montrer, à l'aide du théorème de Wilson, que $x^2 \equiv -1 \pmod p$.

(b) En appliquant le lemme de Thue à x, montrer que p peut s'écrire comme somme de deux carrés.

On a donc démontré le *théorème des deux carrés* :

Théorème 2 (Théorème des deux carrés). *Un nombre premier $p \geqslant 3$ peut s'écrire comme somme de deux carrés si et seulement si $p \equiv 1 \pmod 4$.*

3 Partie 3 : l'algorithme de Serret

1°. Soient $x > 1$ entier et $p \geqslant x$ premier. A partir des suites finies (q_k) et (r_k), avec $r_0 = p$ et $r_1 = x$, des quotients et restes successifs obtenus par l'algorithme d'Euclide (pour le calcul de $\text{pgcd}(p, x)$), on définit les suites (s_k) et (t_k) pour tout entier $1 \leqslant k \leqslant n$ par :

$$\begin{cases} s_0 = 1, s_1 = 0, & s_{k+1} = -q_k s_k + s_{k-1} \\ t_0 = 0, t_1 = 1, & t_{k+1} = -q_k t_k + t_{k-1}. \end{cases}$$

(a) Montrer que, pour tout entier $0 \leqslant k \leqslant n+1$, on a $r_k = s_k p + t_k x$.

(b) Montrer que, pour tout entier $0 \leqslant k \leqslant n+1$, on a $s_k = (-1)^k |s_k|$ et $t_k = (-1)^{k+1} |t_k|$. En déduire que, pour tout entier $1 \leqslant k \leqslant n$, on a :

$$|s_{k+1}| = q_k |s_k| + |s_{k-1}|$$
$$|t_{k+1}| = q_k |t_k| + |t_{k-1}|.$$

(c) En déduire que, pour tout entier $1 \leqslant k \leqslant n+1$, on a :

$$p = |t_k| r_{k-1} + |t_{k-1}| r_k.$$

2°. Soient $x > 1$ entier et $p > x$ premier et soit (r_k) la suite finie des restes successifs fournis par l'algorithme d'Euclide (pour le calcul de $\text{pgcd}(p, x) = 1$).

(a) Expliquer pourquoi il existe un entier $k \geqslant 1$ tel que $r_{k-1} > \sqrt{p} \geqslant r_k$.

(b) En utilisant les questions 1°c et 1°a, montrer que le couple $(u, v) = (t_k, r_k)$ vérifie les conditions du Lemme de Thue.

3° **Exemple.** Ecrire $p = 9733$ comme somme de deux carrés.