Ateliers de découverte en arithmétique
deuxième université d'été européenne, juillet 1999
par E.Cousquer (USTL)

Dans cet atelier a été présentée une expérience intitulée "Atelier mathématique" en première année d'université. Cet enseignement se déroule à raison de deux heures par semaine pendant le premier semestre. On propose aux étudiants d'expérimenter, de conjecturer des résultats et de les démontrer. Cet article présente quelques uns des ateliers, résume la progression adoptée, donne un aperçu des fiches de travail pour les étudiants et les références de textes historiques liés à ces ateliers. En conclusion, l'intérêt de l'histoire pour l'élaboration de ces ateliers est analysée.

Atelier 1 : Nombres premiers

Il s'agit dans ce premier atelier d'explorer librement les nombres premiers, la décomposition en facteurs premiers et quelques autres propriétés, en utilisant les théorèmes établis par Euclide et Gauss, et le crible d'Eratosthène. On fournit ou non aux étudiants les textes historiques correspondants d'Euclide, de Gauss ou de Nicomaque de Gérase. Si non, on peut expliquer brièvement les méthodes.

Textes historiques fournis à l'Université d'été

— les propositions 31 à 34 du livre 7 des "Éléments" d'Euclide sur les nombres premiers et les nombres composés.
— la proposition 20 du livre 9 des "Éléments" d'Euclide, *Les nombres premiers sont en quantité plus grande que toute quantité composée de nombres premiers*.
— le texte de Nicomaque de Gérase sur le crible d'Erathostène (dans "Introduction arithmétique" livre I Chapitre XIII) dont on trouve un extrait dans le livre "Mathématiques au fil des âges". (p 54 et 55).
— Les deux premières pages de la section seconde des "Recherches arithmétiques" de Gauss avec en particulier le théorème 16 : *Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers*

Travail pour les étudiants

La fiche de travail comporte une série de tableaux à remplir, de conjectures à formuler et de démonstrations à faire. D'abord, les étudiants doivent faire le crible pour des entiers de 1 à 200 sur un tableau du modèle suivant :

Crible d'Ératosthène

	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
$\ddots$					
199	200				

entier p dont on barre les multiples	nombre de multiples de p	multiples non déjà barrés
2		
3		
$\ddots$		

Pour quelle valeur P de p est-on sûr d'avoir obtenu uniquement des nombres premiers ? Pourquoi ? *Il s'agit de faire redécouvrir que si on veut programmer le crible de* 1 *à* N*, on s'arrête quand on a atteint l'entier immédiatement inférieur à* $\sqrt{N}$.

Pourquoi la disposition utilisée dans le crible est-elle intéressante ? Quelles conjectures peut-on faire sur les nombres premiers à partir de cette étude ? *Les nombres premiers supérieurs à* 3 *se répartissent dans deux colonnes, ceux du type* $6k + 1$ *et ceux du type* $6k - 1$.

Infinité de nombres premiers

On reprend la démonstration d'Euclide : Supposons que nous connaissions seulement un nombre fini de nombres premiers p_1, p_2, ..., p_i. Montrons qu'on peut trouver un autre nombre premier. On considère l'entier $N = p_1 \times p_2 \times ... \times p_i + 1$. Il est facile de voir qu'il n'est divisible par aucun des nombres premiers p_1, p_2, ..., p_i. Si N est premier, nous avons trouvé un nombre premier qui n'est pas dans la liste initiale. Si N n'est pas premier, il possède un diviseur premier q qui n'est pas dans la liste initiale. Conclusion : La liste des entiers premiers n'est pas finie.

Consignes de travail

— Calculer les entiers premiers obtenus quand on prend successivement i de 1 à 10, en utilisant un logiciel de décomposition en facteurs premiers. *On demande ici d'abord de prendre les entiers premiers successifs et de voir les nombres premiers qui apparaissent comme plus petits diviseurs. On peut aussi rester plus proche du texte d'Euclide, prendre* $p_1 = 2$, $p_2 = 3$, $p_3 = 7, \cdots$ *On constate que les nombres augmentent très vite, d'où la nécessité de disposer de calculatrices formelles ou d'un logiciel de décomposition en facteurs premiers.*

— Démontrer qu'il existe une infinité de nombres premiers dans la colonne 5 du crible, en calquant l'argument d'Euclide sur l'existence d'une infinité de nombres premiers. *On suppose qu'on a déjà trouvé une famille finie* p_1, p_2, $\cdots$, p_n *de tels entiers. On considère l'entier* $M_n = 6p_1p_2 \cdots p_n - 1$ *; on le décompose* *en facteurs premiers, on montre que l'un de ces facteurs au moins est du type $6k - 1$, et on désigne par p_{n+1} le plus petit de ces facteurs du type $6k - 1$, en ayant justifié qu'il ne figure pas dans la liste précédente. On fait calculer la liste des 5 premiers nombres premiers ainsi obtenus.*

On fait démontrer ici un cas particulier simple du théorème de Lejeune - Dirichlet qui affirme qu'il existe une infinité de nombres premiers dans toute progression arithmétique du type $an + b$ avec a et b entiers premiers entre eux.

Atelier 2 : Fractions irréductibles

Il s'agit de s'entraîner à utiliser des décompositions en facteurs premiers pour simplifier des fractions. On va lister les fractions irréductibles de dénominateurs petits et les compter. Pour cela, on va s'inspirer du crible d'Eratosthène pour compter pour chaque dénominateur n le nombre $\Phi(n)$ de numérateurs sans facteurs premiers commun avec ce dénominateur. On va apprendre à le calculer pour des petites valeurs.

Ici, on découvre un mode de calcul de la fonction d'Euler à partir de la décomposition du nombre n en facteurs premiers, que l'on peut justifier assez facilement jusqu'à trois facteurs premiers. On disposera donc de cette fonction pour de petites valeurs de n dans les ateliers suivants et on reviendra dans un atelier ultérieur sur cette fonction et ses propriétés.

Travail à faire

Barrer les numérateurs qui ne conviennent pas. Compter les fractions irréductibles. (On présente ici un extrait du tableau qui demande de trouver toutes les fractions irréductibles pour des dénominateurs de 2 à 30)

Dénominateur	Facteurs premiers du dénominateur	Numérateurs des fractions irréductibles	Nombre de fractions irréductibles
$\ddots$			
12	$2, 3$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ $11, 12$	
13	13	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ $11, 12, 13$	
14	$2, 7$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ $11, 12, 13, 14$	
$\ddots$			

Fractions irréductibles : conjectures sur $\Phi(n)$

$nombre$ n	$p_1^{\alpha_1}$	$p_2^{\alpha_2}$	$p_3^{\alpha_3}$	$\Phi(p_1^{\alpha_1})$	$\Phi(p_2^{\alpha_2})$	$\Phi(p_3^{\alpha_3})$	$\Phi(n)$
$\ddots$							
12							
13							
14							
$\ddots$							

Conjectures :
Que se passe-t-il si n est premier ?
Que se passe-t-il si n est une puissance d'un nombre premier ?
Que se passe-t-il si n admet deux nombres premiers dans sa décomposition ?
Essayer de démontrer ces conjectures.

Textes historiques fournis

On a renvoyé à une présentation détaillée de l'introduction de la fonction d'Euler par Gauss qui se trouve dans le livre "La fabuleuse histoire des nombres" et fourni l'extrait suivant.

Extrait

Calculer le nombre de fractions irréductibles de dénominateur p revient au problème suivant [1] posé par Gauss :

> *«Trouver combien il y a de nombres plus petits qu'un nombre donné*
> *A et premiers avec lui ?»*

Désignons ce nombre par $\phi(A)$. Gauss examine les différents cas :

– Quand A est un nombre premier p, il est évident que

$$\phi(p) = p - 1$$

– Quand $A = p^m$, pour obtenir $\phi(A)$ il faut retrancher à A le nombre d'entiers inférieurs à A divisible par p, c'est à dire A/p, ce qui donne

$$\phi(p^m) = p^m - p^{m-1} = p^m(1 - \frac{1}{p})$$

[1] *Disquisitiones arithmeticae* (1801) paragraphe 38

– Quand A est décomposé en facteurs premiers entre eux $M \times N \times P...$ alors Gauss montre que

$$\phi(A) = \phi(M) \times \phi(N) \times \phi(P) \times ....$$

Gauss applique ensuite cette relation au cas où A est décomposé en facteurs premiers :

$$A = a^\alpha b^\beta c^\gamma \Longrightarrow \phi(A) = A(1 - \frac{1}{a})(1 - \frac{1}{b})(1 - \frac{1}{c})...$$

Un exemple pour comprendre : Cherchons le nombre de fractions irréductibles de dénominateur $18 = 2 \times 3^2$: On écrit les nombres de 1 à 18, on enlève les $18/2$ multiples de 2, on enlève les $18/3$ multiples de 3, mais on a retiré deux fois les multiples de 6, on doit donc rajouter $18/6$.

$$\phi(18) = 18 - \frac{18}{2} - \frac{18}{3} + \frac{18}{6} = 18(1 - \frac{1}{2})(1 - \frac{1}{3})$$

Si nous écrivons les 18 fractions de dénominateurs 18, après simplification, elles se répartissent en fractions ayant pour dénominateurs les différents diviseurs de 18.

$\frac{1}{18}$	$\frac{2}{18}$	$\frac{3}{18}$	$\frac{4}{18}$	$\frac{5}{18}$	$\frac{6}{18}$	$\frac{7}{18}$	$\frac{8}{18}$	$\frac{9}{18}$	$\frac{10}{18}$	$\frac{11}{18}$	$\frac{12}{18}$	$\frac{13}{18}$	$\frac{14}{18}$	$\frac{15}{18}$	$\frac{16}{18}$	$\frac{17}{18}$	$\frac{18}{18}$
																	1
								$\frac{1}{2}$									
					$\frac{1}{3}$						$\frac{2}{3}$						
		$\frac{1}{6}$												$\frac{5}{6}$			
	$\frac{1}{9}$		$\frac{2}{9}$				$\frac{4}{9}$		$\frac{5}{9}$				$\frac{7}{9}$		$\frac{8}{9}$		
$\frac{1}{18}$				$\frac{5}{18}$		$\frac{7}{18}$				$\frac{11}{18}$		$\frac{13}{18}$				$\frac{17}{18}$	

Si on compte les fractions sur chaque ligne [2] on obtient [3] :

$$18 = \phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(9) + \phi(18)$$

Nous avons introduit là la *fonction d'Euler* dont Gauss cite deux articles en référence [4]. Gauss démontre [5] le résultat que nous avons illustré avec notre tableau : *Si a, a', a'' sont tous les diviseurs de A* [6]*, on aura :*

$$A = \phi(a) + \phi(a') + \phi(a'') + ...$$

Atelier 3 : Suites F_n de fractions irréductibles

On considère des suites finies des fractions définies de la façon suivante : F_n est l'ensemble des fractions irréductibles $\frac{a}{b}$, comprises entre 0 et 1, avec $0 \leq a$, $0 < b \leq n$, rangées par ordre de grandeur croissante.

Exemples :

$$F_1 = (\frac{0}{1}, \frac{1}{1})$$

$$F_2 = (\frac{0}{1}, \frac{1}{2}, \frac{1}{1})$$

$$F_3 = (\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1})$$

$$F_4 = (\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1})$$

$$F_5 = (\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1})$$

Activités proposées : Construire les suites F_n d'ordre inférieur ou égal à 10. Émettre des conjectures concernant ces suites. Démontrer ensuite ces conjectures.

---

[2] Cette méthode n'est pas dans le livre de Gauss, mais elle nous paraît très éclairante.

[3] en posant $\phi(1) = 1$.

[4] *Theoremata arithmetica nova methodo demonstrata* comment. nov. acc.Petrop. VIII page 74 et *Speculationes circa quasdam insignes proprietates numerorum* Acta Patrop. VIII p 17.

[5] paragraphe 39.

[6] 1 y compris.

Les suites de Farey

On exploite ici une curiosité mathématique dénommée les suites de Farey pour retrouver d'une manière différente les théorèmes de Bézout et de Gauss. Cet atelier peut être considéré comme un atelier de travail sur le raisonnement par récurrence. Il est très difficile pour les étudiants qui n'ont pas l'habitude de faire des raisonnements un peu complexes. C'est une façon de retravailler l'arithmétique élémentaire sans refaire un cours classique.

Le premier mathématicien a avoir démontré des résultats semble être Haros qui démontre en 1802 que si on a trois fractions successives a/b, c/d, e/f d'une suite de Farey, alors $c/d = (a+c)/(b+f)$. Il montre que si on a deux fractions successives a/b et c/d, alors $bc - ad = 1$. Il semble que Farey ait énoncé sans démonstration dans un article en 1816 un de ces résultats et que Cauchy qui lut l'article, donna une démonstration de ce résultat et nomma ces suites du nom de Farey.

Textes historiques fournis

— texte original de Bézout ("Cours de mathématique à l'usage des Gardes...") reproduit dans le livre "Histoire d'algorithmes" p140 et suivantes.
— deux extraits de Pascal ("Traité de triangle arithmétique") et de Poincaré ("La science et l'hypothèse") sur le raisonnement par récurrence

Guide de travail

Conjectures sur les suites F_n

Vérifier pour ces suites F_1 à F_{10} les propriétés A et B suivantes :
Propriété A : Si $\frac{a}{b}$ et $\frac{c}{d}$ sont des termes consécutifs d'une suite F_n, alors $bc-ad = 1$ et $b + d \geq n + 1$.
Propriété B 1 : Si $\frac{a}{b}$ et $\frac{c}{d}$ sont des termes consécutifs d'une suite F_n et si $b + d > n + 1$, alors $\frac{a}{b}$ et $\frac{c}{d}$ sont des termes consécutifs de la suite F_{n+1}.
Propriété B 2 : Si $\frac{a}{b}$ et $\frac{c}{d}$ sont des termes consécutifs d'une suite F_n et si $b + d = n + 1$, alors $\frac{a}{b}$, $\frac{a+c}{b+d}$ et $\frac{c}{d}$ sont des termes consécutifs de la suite F_{n+1}.
Propriété B 3 : Si $\frac{a}{b}$, $\frac{c}{d}$ et $\frac{e}{f}$ sont des termes consécutifs d'une suite F_n alors $\frac{c}{d} = \frac{a+e}{b+f}$.

Propriétés préliminaires de fractions

Démontrer les propriétés C et D suivantes, (utiles pour démontrer les propriétés A et B).
Propriété C 1 : Si $bc - ad = 1$, alors $\frac{a}{b}$ et $\frac{c}{d}$ sont irréductibles.

Propriété C 2 : Si $\frac{p}{q}$ vérifie $\frac{a}{b} \leq \frac{p}{q} \leq \frac{c}{d}$, alors $\frac{p}{q}$ s'écrit $\frac{ax+cy}{bx+dy}$, où x et y sont des entiers positifs ou nuls.
Propriété D 1 : Toute fraction irréductible comprise entre $\frac{a}{b}$ et $\frac{c}{d}$ et non identique à l'une d'elles, est de la forme $\frac{ax+cy}{bx+dy}$, où x et y sont des entiers positifs non nuls, et a donc un dénominateur supérieur ou égal à $b+d$.
Propriété D 2 : Si $bc-ad=1$, alors la fraction $\frac{p}{q} = \frac{a+c}{b+d}$ est irréductible et vérifie : $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$

Démonstrations des propriétés des fractions F_n

Démontrer les propriétés A et B, par récurrence sur n. En déduire les règles de formation de F_{n+1} à partir de F_n.

Ateliers 4, 5, 6 : sur les développements illimités de rationnels

Le travail fait sur les développements illimités de rationnels en liaison avec l'étude des "Recherches arithmétiques" de Gauss a été présenté à Louvain.

Activité proposée

Le développement décimal d'un rationnel comporte une partie entière suivie d'une partie fractionnaire. On s'intéressera à la seule partie fractionnaire, ce qui revient à s'intéresser aux fractions irréductibles, entre 0 et 1, c'est-à-dire aux fractions dont le numérateur est inférieur au dénominateur. La partie fractionnaire comporte une partie périodique de i chiffres, précédée d'un certain nombre n de chiffres. On se propose de chercher si l'on peut trouver des lois générales sur le nombre i de chiffres de la période, et sur le nombre n de chiffres précédant la partie périodique du développement, en fonction des entiers p et q.

Calculer le développement périodique illimité des fractions $\frac{p}{q}$ irréductibles, inférieures à 1, ($p < q$), pour q variant par exemple de 3 à 17. Déterminer les nombres n et i correspondant à chacune des fractions et essayer d'émettre des conjectures, sur les nombres n et i.

Trouver un critère pour grouper les développements des fractions de dénominateur q en familles. Combien trouve-on de familles ? Là-aussi, on peut émettre des conjectures et essayer de les démontrer. Tester les conjectures obtenues sur les fractions de dénominateurs compris entre 19 et 29.

Commentaires sur cette activité

C'est une activité très riche qui permet de découvrir les propriétés des rationnels, de travailler les congruences, le petit théorème de Fermat et plus généralement la formule d'Euler. On voit apparaître également la notion de racine primitive. Ces activités et l'analyse des chapitres correspondants du livre de Gauss sont publiées dans le livre "La fabuleuse histoire des nombres" ; cette étude ne sera donc pas reprise ici.

Cette activité a été d'abord élaborée pour un stage de formation continue d'enseignants, en partant d'une indication trouvée dans le livre de Hardy et Wright. Elle a fait l'objet d'un mémoire professionnel de seconde année d'IUFM, où les professeurs stagiaires avaient fait des programmes pour déterminer entre autres les nombres n et i. C'est seulement ensuite l'histoire a été abordée avec l'étude des "Recherches arithmétiques" ; il est frappant que ce texte de Gauss ait éclairé les difficultés rencontrées dans la programmation.

L'activité présentée ici est fidèle à un aspect des recherches de Gauss qui a beaucoup expérimenté sur des valeurs particulières, par exemple en confectionnant des tables de valeurs, avant d'induire des résultats qu'il démontrait ensuite (ou pour lesquels il indiquait ne pas avoir encore une démonstration générale). La méthode utilisée ici présente donc aussi un intérêt historique.

La méthode de Gauss

L'ouvrage de Gauss, (1777-1855), les *Disquisitiones arithmeticae* (1801) a marqué un tournant dans l'histoire de l'arithmétique. On y trouve dans la troisième section la théorie des congruences , et dans la sixième sont développées différentes applications dont la théorie des développements décimaux illimités figure pages 388 à 398 de la traduction du livre de Gauss paru aux éditions Blanchard sous le titre *Recherches Arithmétiques*.

Contexte historique

Le problème de Gauss était de fournir un moyen de calculer tous les développements décimaux illimités de fractions de dénominateurs premiers inférieurs à 100, avec le minimum de calculs. (Penser à l'absence alors de moyens de calculs !) Il a découvert que pour une valeur fixée du dénominateur q, les périodes des développements se groupaient par familles. Si 10 était une racine primitive modulo q, c'est-à-dire si ses puissances engendrent tous les résidus non nuls, alors les différentes périodes peuvent être obtenues à partir d'une seule, par permutation circulaire. Mais si 10 n'est pas racine primitive, Gauss montre comment utiliser d'autres racines primitives pour obtenir tous les développements à partir de quelques uns. Il est amené à établir une table de racines primitives, à développer une théorie des indices qui sont une sorte de logarithme.

Cette question des racines primitives a été beaucoup étudiée après Euler et Gauss. Des tables de racines primitives ont été établies, par exemple par Jacobi en 1839 pour tous les entiers premiers jusqu'à 1000, par Cunningham en 1900, pour les entiers premiers jusqu'à 10000 et la course ne s'est pas arrêtée là... On trouve une étude historique très complète sur les racines primitives et les congruences dans le deuxième chapitre du livre de Dickson sur l'histoire de la théorie des nombres , *History of the theory of numbers*.

Analyse du texte de Gauss

Lorsque l'on fait une lecture linéaire du texte de Gauss, les passages du chapitre trois sur la recherche de racines primitives sont très difficiles à comprendre, car beaucoup d'arguments sont des arguments ad hoc, tirés d'une pratique. Tout s'éclaire lorsque l'on part des tables I (racines primitives) et III (périodes de développements) qui sont à la fin du livre et si on commence à faire soi-même les calculs pour établir de telles tables. On a alors un exemple particulièrement évident d'une écriture a posteriori du chapitre trois, faite pour expliquer les méthodes employées pour réaliser ces tables.

Intérêt historique

Le contexte a changé et l'existence de moyens de calculs puissants rend caduque le problème posé par Gauss d'établir des tables commodes. Mais la théorie établie à cette occasion est tout à fait d'actualité. Toute cette théorie n'est pas une curiosité historique et les idées développées dans ce chapitre sont très importantes dans les théories du codage. Bien sûr, la théorie des développements décimaux n'est pas centrale dans les recherches mathématiques actuelles. Elle a l'avantage de faire aborder ces questions d'une façon simple et naturelle.

La théorie des congruences telle qu'elle figure dans Gauss, sans utiliser du tout le langage des structures algébriques est intéressante au niveau pédagogique : cela peut aussi être une étape dans l'enseignement où au lieu d'utiliser la formalisation la plus récente, on fait les démonstrations dans le langage des congruences, avant de parler de groupes finis.

Ateliers suivants

Le thème suivant des ateliers porte sur l'étude des racines de l'unité, des sous-groupes et des polynômes associés à ces racines. Un premier atelier fait découvrir ces questions successivement pour les racines troisièmes, sixièmes, douzièmes et vingt-quatrièmes de l'unité. On fait placer ces racines sur le cercle, étudier les sous-groupes engendrés par les différentes racines et on dégage la notion de racine primitive n-ième de l'unité. Les étudiants découvrent avec surprise que l'arithmétique apparaît à propos de ces questions sur des nombres complexes. À partir de là, on fait travailler en atelier les nombres de Mersenne et les polynômes cyclotomiques.

En conclusion

L'histoire a été un moyen puissant pour découvrir des problématiques et des méthodes de travail à proposer aux étudiants dans ces ateliers.

Aujourd'hui avec l'introduction des outils de calculs formels, on parle beaucoup d'introduction de méthodes expérimentales en mathématiques. En fait, l'étude de Gauss montre qu'il s'agit tout simplement de mettre les étudiants dans la posture d'avoir une activité mathématique réelle qui ne soit pas une simple reproduction d'un discours. On a oublié, depuis la vague formaliste dans l'enseignement qu'il y a autre chose qu'un exposé linéaire et axiomatique des mathématiques, qui, s'il est utile pour celui qui a déjà une pratique d'un domaine, pour clarifier, dégager les idées générales et vérifier les cohérences, restent souvent pour les débutants à l'état de discours qu'on apprend et qu'on oublie.

La difficulté pour une autre forme d'enseignement est de trouver des problématiques suffisamment riches pour être signifiantes mathématiquement, et abordables par les débutants. L'intérêt des activités élaborées à partir de l'histoire est que les moyens de calculs actuels permettent d'avoir très vite des résultats signifiants qui permettent aux étudiants d'élaborer des conjectures et d'essayer de les démontrer. Une leçon à tirer de cette expérience est que l'intérêt manifesté par les étudiants pour cette activité de recherche ne doit pas faire sous-estimer la difficulté de leur faire rédiger des démonstrations à partir de là. C'est un exercice très formateur, car il ne s'agit pas de répondre à des questions du type 1a suivie de 1b etc ..., mais de mettre en ordre, de dégager ce qu'on doit démontrer, les prémisses dont on dispose. C'est l'autre volet de l'activité du mathématicien : communiquer ce qu'il a trouvé.

Bibliographie

Collectif, *Arithmétique, secrets des nombres*, dans "Tangente", Éditions Archimède, hors série 1998.

Collectif, *Autour de l'algorithme d'Euclide*, *Algorithmes de l'arithmétique*, dans "Histoire d'algorithmes", Belin, 1994, 20 pages.

Collectif, *Les nombres*, Vuibert, 1998, 432 pages.

Conway, *The book of numbers*, Springer - Verlag, 1996, 310 pages.

Cousquer, *La fabuleuse histoire des nombres*, Édition Diderot, 1998, 265 pages.

Crubellier, Sip, *A la recherche des nombres parfaits,* dans "Histoire de problèmes, histoire des mathématiques", Ellipses, 1993, 20 pages.

De Koninck, Mercier, *Introduction à la théorie des nombres* , collection Modulo 1994.

Demazure, *Cours d'algèbre, primalité, divisibilité*, *codes*, Éditions Cassini 1997.

Dickson, *History of numbers* , Chelsea publishing company.

Gauss, *Recherches arithmétiques, (Disquisitiones arithmeticae)* , Réédition Blanchard 1979.

Guinot, *Arithmétique pour amateurs, Pythagore, Euclide et toute la clique*, *Arithmétique pour amateurs, les resveries de Fermat*, *Ce diable d'homme d'Euler*, *Une époque de transition*, Aleas Editeur, Lyon, 1992 et années suivantes, série de livres.

Hardy, Wright, *An introduction to number theory*, Oxford university press, 1960.

Jaboeuf, *Les nombres premiers*, dans "Histoire de problèmes, histoire des mathématiques", Ellipses, 1993, 30 pages.

Oystein Ore, *Number theory and its history*, Éditions Dover (1988) réédition d'un livre de 1948.

Rashed, *Analyse combinatoire, analyse numérique, analyse diophantienne et théorie des nombres*, "Histoire des mathématiques arabes", Seuil, 1997, 38 pages.

Saidan, *Numération et arithmétique*, "Histoire des mathématiques arabes", Seuil, 1997, 20 pages.

Silvermann, *A Friendly Introduction to Number Theory*, Éditions Prentice Hall (19887).