I.R.E.M

DE

POITIERS

ARITHMETIQUE au FIL des AGES.

MAI 1984

Recueil de textes destinés à constituer le
chapitre ARITHMETIQUE du livre
" Textes Mathématiques au Fil des Ages "
préparé par le commission inter-IREM
d'histoire et d'épistémologie des Mathématiques.

Roger CUCULIERE
Jean-Paul GUICHARD

Il s'agit d'un ouvrage de 350 pages environ présentant des pages choisies de textes mathématiques considérés comme classiques et de textes importants sur les mathématiques. Ces extraits ont une longueur variant de 2 à 5 ou 6 pages maximum, et sont accompagnés de commentaires introductifs et de quelques notes destinés à en faciliter la lecture. Le volume de ces notes n'excéde pas le quart du volume total de l'ouvrage.

Cet ouvrage est destiné à être utilisé dans les classes de Premières et Terminales des lycées conformément aux instructions des programmes officiels de l'Education Nationale lesquels suggèrent l'introduction de l'histoire des mathématiques, notamment dans les classes littéraires. Ces textes pourraient être étudiés dans les classes par les professeurs de mathématiques, de philosophie et d'histoire et offrir ainsi l'occasion de collaboration entre plusieurs disciplines. Néanmoins, cet ouvrage devrait intéresser un public beaucoup plus large que celui des lycées, car il va présenter, de façon rassemblée, des textes dont l'accès est souvent très difficile, soit parce qu'il s'agit de textes anciens non réédités depuis très longtemps, soit parce qu'il s'agit de textes jamais traduits en français. L'intérêt très vif que rencontre l'histoire des sciences ces dernières années à tous les niveaux nous semble justifier la parution d'un tel ouvrage aujourd'hui.

IREM de Poitiers
40, Avenue du Recteur Pineau
86022 - POITIERS CEDEX

1 - PRESENTATION.

Texte 1 : Anatolius : la nature et les beautés des dix premiers nombres.

Texte 2 : Legendre : panorama de la théorie des nombres en 1830.

2 - LES DEBUTS DE L'ARITHMETIQUE.

Texte 3 : Nicomaque de Gérase : nombres figurés.

Texte 4 : Nicomaque de Gérase : crible d'Erathostène, nombres premiers et premiers entre eux.

Texte 5 : Euclide : algorithme du PGCD.

Texte 6 : Euclide : un exemple de démonstration par descente infinie et la décomposition d'un nombres en facteurs premiers.

Texte 7 : Euclide : l'infinité des nombres premiers.

3 - NUMERATION.

Texte 8 : Stevin : les nombres décimaux + iconographie.

Texte 9 : Pascal : les caractères de divisibilité.

Texte 10 : Leibniz : arithmétique binaire.

4 - LE RENOUVEAU.

Texte 11 : Fermat : la descente infinie.

Texte 12 : Legendre : la réciprocité quadratique.

Texte 13 : Gauss : les congruences.

5 - VERS LES FONDEMENTS.

Texte 14 : Leibniz : deux plus deux égale quatre.

Texte 15 : Frege : peut-on démontrer les formules numériques ? + iconographie (une page de Peano).

Texte 16 : Poincaré : le raisonnement par récurrence + un encadré (Pascal).

6 - PROBLEMES.

Texte 17 : Diophante : un système du second degré.

Texte 18 : Nicomaque de Gérase : génération des cubes.

Texte 19 : Bachet : un problème plaisant du premier degré.

Texte 20 : Fermat : un testament.

Texte 21 : Collatz : le problème de Syracuse.

7 - POUR EN SAVOIR PLUS.

1 - PRESENTATION.

Platon dans la République (voir généralités) cherchait quelles sont les sciences " que chacun doit apprendre parmi les premières ". Nicomaque de Gérase dans le début de son Introduction arithmétique reprend le problème du choix entre arithmétique, géométrie, musique, sphérique et astronomie, posé par Platon : " Laquelle de ces quatre méthodes faut-il donc apprendre en premier ? N'est-ce pas évidemment celle qui par nature préexiste à toutes les autres et qui est plus souveraine, parce qu'elle tient le rôle de principe, de racine, et pour ainsi dire de mère pour les autres ? ". Il s'agit bien sûr de l'arithmétique. De même de nos jours les fondements de l'édifice mathématique reposent en dernière analyse sur ceux de l'ensemble des entiers naturels : la crise des fondements a été marquée par la définition du nombre (ordinal et cardinal), l'axiomatisation de N et le problème de la non contradiction de l'arithmétique. Mais ce que l'on entend par arithmétique a beaucoup varié et évolué au fil des âges et il est difficile de cerner son champ tant sont étroits ses liens avec le calcul (la logistique des anciens), l'algèbre et l'analyse (voir le panorama de Legendre t.12). Nous avons essayé de rester au coeur de l'arithmétique dont la spécificité réside peut-être dans le charme et la nature de ses problèmes : problèmes aux énoncés souvent très simples, sur des objets simples, qui incitent à la recherche mais dont les solutions nous entrainent dans le labyrinthe du monde mystérieux des nombres.

Texte 1 : Anatolius : la nature et la beauté des dis premiers entiers.

Anatolius . Sur la décade et les nombres qu'elle comprend, traduit par Paul Tannery dans Mémoires Scientifiques III, p. 12-28 à partir du texte grec reconstitué par J.-L. Heiberg et publié dans Annales internationales d'histoire (Congès international d'histoire comparée de 1900, 5è section, p. 27-41.

La nature de la décade et des nombres qu'elle comprend présente mille beautés évidentes pour ceux dont l'intellect perspicace est capable d'une telle contemplation. Nous en dirons autant qu'il sera possible sur chacun de ces nombres; pour le moment et comme préambule, il suffit de remarquer que les Pythagoriens ont ramené tous les nombres à dix et qu'au-dessus de dix il n'y a plus de nombre nouveau, puisque, quelle que soit l'augmentation, dès qu'une dizaine est complétée, nous revenons à l'unité; d'autre part, ils honoraient singulièrement le quaternaire, parce que c'est lui qui constitue la décade $<1+2+3+4=10>$. (...)

L'unité est antérieure à tout nombre ; tous naissent d'elle, elle-même ne naît d'aucun. Aussi est-elle appelée *Semence*, étant la matière des nombres, — car sans elle il n'y a plus de nombre, — indivisible, intransitive, ne sortant point de sa propre nature, même dans les multiplications[1] ; et même, sinon en acte, au moins en puissance, à la fois impaire, paire, pairement impaire, cube, carré, et tout le reste. Elle désigne le point.

Les Pythagoriens l'ont appelée *intellect* et l'ont assimilée à l'Un, au Dieu intelligible, inengendré, Beau et Bien en soi ; (...)

C'est à *deux* que commencent les nombres ; le premier accroissement à partir de l'unité, le premier changement donne le binaire ou le doublement. C'est le premier terme de la série des nombres pairs ; par addition, il équivaut à son propre carré ; car en ajoutant le binaire à lui-même, ou en le multipliant par lui-même, on obtient le même résultat, tandis que, pour les autres nombres, la multiplication donne plus que l'addition. Le binaire désigne la ligne, qui vient après le point ; il est en analogie avec la matière et tout ce qui est sensible. On l'a assimilé, dans la série des Vertus, à la Force, — car il a déjà fait un pas. (...)

Le ternaire provient de l'addition de l'unité au binaire ; c'est le premier nombre impair. Quelques-uns l'appellent *parfait*, parce qu'il est le premier qui signifie le tout, commencement, milieu et fin. Nous l'employons pour mettre en relief ce qui est extraordinaire, comme quand nous disons *trois fois heureux ;* les prières et les libations se répètent trois fois. Le ternaire désigne, en premier lieu, commencement, milieu et fin, puis la surface, qui vient après le point et la ligne ; c'est l'image du plan (...)

Nous assimilons le ternaire, parmi les vertus, à la Tempérance, car elle est la juste mesure entre l'excès et le défaut[2]. (...)

Le quaternaire est appelé Justice, parce que le carré qui en provient a une aire égale à son périmètre, tandis que, pour les nombres qui précèdent, le périmètre du carré est supérieur à l'aire, et que pour ceux qui suivent, le périmètre est inférieur à l'aire. Il est d'ailleurs le premier carré, tant pour tous les nombres que pour les pairs en particulier. C'est la première *tétractys*, puisque la somme des termes consécutifs de 1 à 4 fait 10, qui est dit nombre parfait. C'est le premier nombre qui désigne la nature du solide ; car on a d'abord le point, puis la ligne, puis la surface, puis le solide, c'est-à-dire le corps. On le voit dans le jeu qui consiste à construire des pyramides avec des noix.

Il y a quatre éléments, quatre saisons qui divisent l'année en quatre parties égales. D'autre part, 4 est le premier nombre pairement pair, le premier qui soit à un autre dans le rapport d'un tiers en sus et fournisse la première consonance, celle de quarte. Il présente <comme carré> une égalité complète, entre la valeur de l'aire, le nombre des angles, celui des côtés. Il y a quatre climats <directions>, le levant, le couchant, le septentrion, le midi; quatre points <astrologiques>, celui du levant, celui du couchant, celui du méridien, celui du milieu du ciel[1]; quatre vents principaux. (...)

Le nombre 5 est le premier à renfermer les deux espèces, à savoir le premier pair et le premier impair; car si l'unité est impaire, elle n'est pas nombre. Ainsi 5 provient en longueur, c'est-à-dire par addition, des premiers pair et impair, mâle et femelle; aussi lui donne-t-on cette dernière dénomination. En l'ajoutant à lui-même, on obtient 10, tandis que pour les autres nombres, $1 + 9 = 10$, $2 + 8 = 10$, $3 + 7 = 10$, $4 + 6 = 10$, les termes sont inégaux et ont 5 pour moyen[t]. Si on élève 5 au carré, il reste conservé à la fin du nombre formé, $5 \times 5 = 25$. Si on passe au cube, le carré est conservé en entier et le nombre finit toujours par 5; en effet, $5 \times 25 = 125$.

Il y a cinq figures solides ayant tous leurs côtés égaux et tous leurs angles égaux : le tétraèdre ou pyramide, l'octaèdre, l'icosaèdre, le cube, le dodécaèdre; ce sont d'après *Platon*, les formes respectives du feu, de l'air, de l'eau, de la terre et de l'univers. En dehors du soleil et de la lune, il y a cinq planètes; les cercles parallèles bien connus sur la sphère sont aussi au nombre de cinq, l'équateur, les deux tropiques, le cercle arctique et l'antarctique. Il y a cinq zones, deux glaciales, deux tempérées, une torride. Il y a cinq sens.

Le nombre 6 est le premier parfait; car il est égal à la somme de ses parties aliquotes; $1 + 2 + 3 = 6$, et *une* fois 6 fait 6; *deux* fois 3 font 6; *trois* fois 2 font 6. Il est ainsi le premier qui soit composé d'une moitié, d'un tiers et d'un sixième. (...)

Le sénaire provient par puissance ou multiplication du premier pair et du premier impair, des premiers mâle et femelle; aussi a-t-il été appelé Mâle-femelle, Mariage, Pairement impair. Le nom de Mariage lui vient proprement de ce qu'il est égal, ainsi qu'on l'a vu, à la somme de ses parties, et de ce que l'œuvre du mariage est de produire des enfants semblables aux parents. (...)

Le nombre 7 est le seul qui à la fois n'en engendre aucun autre de la décade et n'est engendré par aucun, sauf l'unité; c'est pourquoi les Pythagoriens l'appellent Vierge sans mère[2], et en effet des autres nombres de la décade, 4 est engendré par 2 et, avec 2, engendre 8; 6 n'engendre pas, mais est engendré par 3; enfin 3 et 5 sont générateurs, 3 de 6 et de 9, 5 de 10. L'addition des sept termes consécutifs de 1 à 7 donne le nombre parfait 28, égal à la somme de ses parties aliquotes. Il y a 28 jours de la lune formant des semaines complètes. (...)

Huit est le premier cube; on l'appelle Solidité et Fondement. Sa racine est le premier pair. Il est la somme de 1 + 3 + 4. La somme des huit premiers nombres en partant de l'unité fait 36, nombre de jours pendant lesquels prennent forme, dit-on, les embryons des enfants qui naissent à sept mois. La sphère qui renferme l'univers est la huitième, d'où le proverbe : Huit est tout. (...)

Neuf est le premier carré du premier impair, comme 4 l'est du premier pair. Les neuf premiers nombres à partir de l'unité donnent comme somme 45; c'est le nombre de jours nécessaire, dit-on, pour que prennent forme les embryons des enfants qui naissent à neuf mois. La terre est la neuvième sphère autour de laquelle tournent les huit autres. (...)

Dix est engendré, par multiplication, d'un pair et d'un impair; car 5 × 2 = 10. C'est le cercle et la limite de tout nombre, car c'est à lui que nous tournons et revenons en arrière, comme à la borne les coureurs qui doublent le stade. Il est, en effet, la limite pour l'indétermination des nombres; car nous comptons depuis l'unité jusqu'à dix, puis nous disons : dix et un, dix et deux, etc. Quant à vingt, double de dix, il est formé par addition en répétant deux fois les termes dont dix est formé; car si 10 = 1 + 2 + 3 + 4, 20 est la somme de deux fois 1, deux fois 2, deux fois 3, deux fois 4; et de même pour les dizaines suivantes. La décade est surnommée Force et Toute-Parfaite, parce qu'elle limite tout nombre et qu'elle renferme à son intérieur toute nature, pair-impair, muable-immuable, bon-mauvais. On l'appelle aussi *Dikhas*, parce qu'elle reçoit tout[1]. 10 = 4 + 6; mais 10 est aussi la somme des nombres du premier quaternaire, 1 + 2 + 3 + 4. (...)

Texte 2 : Legendre : panorama de la théorie des nombres en 1830.

LEGENDRE : Théorie des nombres 1830. Préface de la première édition, p. VII, VIII, IX.

A EN juger par différents fragments qui nous restent, et dont quelques-uns sont consignés dans Euclide, il parait que les anciens philosophes avaient fait des recherches assez étendues sur les propriétés des nombres. Mais il leur manquait deux instruments pour approfondir cette science : l'art de la numération, qui sert à exprimer les nombres avec beaucoup de facilité, et l'Algèbre, qui généralise les résultats et qui peut opérer également sur les connues et les inconnues. L'invention de l'un et l'autre de ces arts dut donc influer beaucoup sur les progrès de la science des nombres. Aussi voit-on que l'ouvrage de Diophante d'Alexandrie, le plus ancien auteur d'Algèbre qu'on connaisse, est entièrement consacré aux nombres, et renferme des questions difficiles résolues avec beaucoup d'adresse et de sagacité.

Depuis Diophante jusqu'au temps de Viète et Bachet, les mathématiciens continuèrent de s'occuper des nombres, mais sans beaucoup de succès, et sans faire avancer sensiblement la science.

Viète, en ajoutant de nouveaux degrés de perfection a l'Algèbre, résolut plusieurs problèmes difficiles sur les nombres. Bachet, dans son ouvrage intitulé *Problèmes plaisans et délectables*, résolut l'équation indéterminée du premier degré par une méthode générale et fort ingénieuse. On doit à ce même savant un excellent commentaire sur Diophante, qui fut depuis enrichi des notes marginales de Fermat.

Fermat, l'un des géomètres dont les travaux contribuèrent le plus à accélérer la découverte des nouveaux calculs, cultiva avec un grand succès la science des nombres, et s'y fraya des routes nouvelles. On a de lui un grand nombre de théorèmes intéressants, mais il les a laissés presque tous sans démonstration. C'était l'esprit du temps de se proposer des problèmes les uns aux autres. On cachait le plus souvent sa méthode, afin de se réserver des triomphes nouveaux tant pour soi que pour sa nation ; car il y avait surtout rivalité entre les géomètres français et les anglais.

De là il est arrivé que la plupart des démonstrations de Fermat ont été perdues, et le peu qui nous en reste nous fait regretter d'autant plus celles qui nous manquent.

Depuis Fermat jusqu'à Euler, les géomètres, livrés entièrement à la découverte ou à l'application des nouveaux calculs, ne s'occupèrent point de la Théorie des nombres. Euler, le premier, s'attacha à cette partie; les nombreux Mémoires qu'il a publiés sur cette matière dans les Commentaires de Pétersbourg, et dans d'autres ouvrages, prouvent combien il avait à cœur de faire faire à la science des nombres les mêmes progrès dont la plupart des autres parties des mathématiques lui étaient redevables. Il est à croire aussi qu'Euler avait un goût particulier pour ce genre de recherches, et qu'il s'y livrait avec une sorte de passion, comme il arrive à presque tous ceux qui s'en occupent. Quoi qu'il en soit, ses savantes recherches le conduisirent à démontrer deux des principaux théorèmes de Fermat, savoir, 1° que si a est un nombre premier, et x un nombre quelconque non divisible par a, la formule $x^{a-1} - 1$ est toujours divisible par a; 2° que tout nombre premier de forme $4n + 1$, est la somme de deux carrés.

Note : Equation indéterminée du premier degré (dont parle Legendre à propos de Bachet) signifie équation du premier degré à deux inconnues (ax + by = c), qu'il s'agit en arithmétique de résoudre avec des nombres entiers, a, b et c étant eux-même des entiers.

2 - LES DEBUTS DE L'ARITHMETIQUE.

La plupart des propriétés élémentaires des nombres nous sont parvenues dans les livres 7 et 9 des Eléments d'Euclide dont certaines démonstrations, en particulier sur les nombres premiers, figuraient telles quelles il y a peu de temps encore, dans les manuels. Mais c'est de Pythagore et des Pythagoriciens, dont la devise était : " tout est nombres ", que nous viennent les considérations sur le pair et l'impair, les multiples, la classification des nombres selon leurs relations abstraites (nombres premiers, amicaux, parfaits, etc...), les nombres figurés. Et la tradition pythagoricienne a fortement influencé l'enseignement de l'arithmétique jusqu'à la Renaissance. En effet, l'Introduction arithmétique du néopythagoricien Nicomaque de Gérase (IIe siècle après J.C.) eut une influence considérable sur tout l'enseignement mathématique médiéval, principalement à travers l'Institutio arithmètica de Boèce au VIe siècle qui en est une adaptation en latin : ce texte entrait dans le quadrivium, partie essentielle de la formation donnée dans les écoles. Quant à Diophante d'Alexandrie (IIe siècle après J.C.), si aucun texte de lui ne figure ici, c'est que ses recherches sont d'un type différent. Son Arithmétique traiessentiellement de résolution d'équations donc de problèmes que nous qualifierions d'algébriques mais dont certains eurent une grande influence sur le renouveau des recherches arithmétiques avec Bachet de Méziriac et Fermat (voir §4).

Texte 3 : Nicomaque de Gérase : nombres figurés.

Les deux chapitres sur le nombres triangle et le nombre carré extraits de l'Introduction arithmétique de Nicomaque de Gérase font partie d'un ensemble de onze chapitres du livre II consacrés aux nombres figurés (polygônes et polyèdres). On retrouve ces nombres par exemple dans le Traité du triangle arithmétique de Pascal. Ils sont intéressants, en plus des liens qu'ils tissent entre arithmétique et géométrie, dans la mesure où ils permettent l'élaboration de procédés sommatoires. Pascal fait d'ailleurs allusion à ces méthodes des Anciens au début de son petit traité Sommation des puissances numériques.

NICOMAQUE DE GERASE : Introduction arithmétique.
IIe siècle après J.C. Livre II, chapitres VIII et IX.
Traduction J. Bertier Vrin 1978.

Chapitre VIII.

Le nombre triangle.

1) Est donc *triangle* le nombre qui, dans sa résolution en unités, configure en triangle la position équilatérale dans le plan de ses parties ; il a pour exemples :

3, 6, 10, 15, 21, 28,

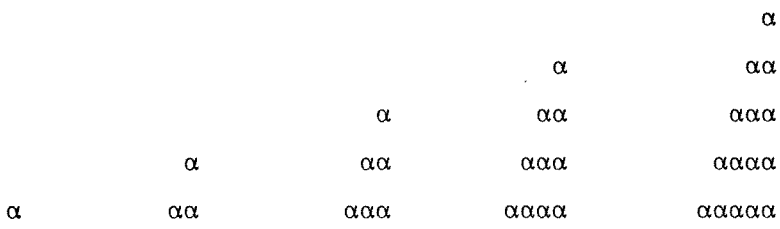
et la suite ; car leurs configuration bien ordonnées seront et *triangles* et équilatérales, et en progressant de cette façon jusqu'où tu voudras, tu trouveras formé en triangle, en rangeant avant tout autre le plus élémentaire, celui qui naît de l'unité, pour que l'unité elle aussi apparaisse *triangle* en puissance, mais le premier *triangle* en acte est le 3.

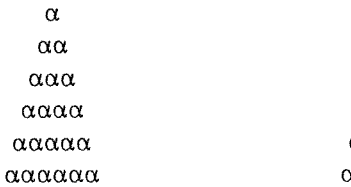
2) Les côtés s'augmenteront du nombre suivant car le côté du premier nombre *triangle* en puissance est l'unité, le côté du premier en acte, le 3, est la dyade, le côté du second en acte, le 6, est la triade, le côté du troisième est la tétrade, celui du quatrième, la pentade, celui du cinquième, l'hexade, et ainsi toujours.

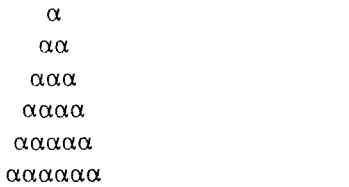
3) Il s'engendre quand le nombre naturel est exposé en ligne et que, toujours depuis le début, les nombres successifs sont ajoutés un à un, car les *triangles* bien ordonnés se réalisent à chaque addition et entassement ; par exemple à partir de cette ligne naturelle :

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.

en prenant le premier nombre, j'ai le premier triangle en puissance, l'unité, ensuite en entassant sur lui le suivant, j'ai le premier *triangle* en acte, car 3 est 2 et 1, et dans la représentation figurée, il se constitue ainsi : sous la première unité on appose deux unités côte à côte, et le nombre 3 est triangulé ; ensuite 3, qui est le nombre suivant, entassé sur ceux-ci, déployé en unités et réuni, produit 6, second nombre *triangle* en acte, et lui donne aussi une configuration ; et à son tour, le nombre qui suit naturellement, 4, entassé sur ceux-ci et noté en unités, donne le nombre 10, bien ordonné après ceux dont on vient de parler, et il prend un configuration triangulaire ; et 5 après lui, puis 6, puis 7, et tous les suivants, de sorte que les côtés de chacun compteront harmonieusement autant d'unités que de nombres de la ligne naturelle réunis pour sa constitution.







Chapitre IX.

Le nombre tétragone.

1) Est *tétragone* le nombre qui vient après celui-ci et qui donne, non plus trois angles comme le précédent, mais quatre angles dans la représentation figurée, pourtant lui aussi dans une configuration équilatérale, comme :

1, 4, 9, 16, 25, 36, 49, 64, 81, 100,

car leurs tracés équilatéraux deviennent des *tétragones* de la façon suivante :

α	αα	ααα	αααα	ααααα
	αα	ααα	αααα	ααααα
		ααα	αααα	ααααα
			αααα	ααααα
				ααααα

et ainsi de suite jusqu'où tu veux.

2) Il advient à ces nombres, comme à ceux qui les précèdent, que la progression des côtés suit le nombre naturel ; car dans le premier en puissance un, l'unité est côté, dans le premier en acte, 4, la dyade est côté, dans le second en acte, 9, la triade est côté, dans le suivant, le troisième en acte, 16, la tétrade est côté, dans le quatrième, le pentade, dans le cinquième, l'hexade, et d'une façon générale ainsi de suite pour les suivants.

3) Celui-ci aussi s'engendre quand le nombre naturel qui s'étend par l'unité est exposé en ligne, en entassant non plus les suivants sur les suivants, comme il a été montré, mais toux ceux qui sont distants de un les uns des autres, c'est-à-dire les *impairs* ; car le premier est 1, premier *tétragone* en puissance, le second 1 et 3, premier *tétragone* en acte, le troisième 1, 3 et 5, second *tétragone* en acte, le quatrième 1, 3, 5 et 7, troisième *tétragone* en acte, et le suivant naît de l'entassement de 9 sur les précédents, et celui qui vient après lui, de celui de 11, et ainsi toujours.

4) Il arrive à ces nombres que le côté de chacun compte autant d'unités qu'il y a de nombres entassés pour sa génération.

Note : pour bien comprendre la différence entre nombre triangle en puissance et en acte on se reportera à la définition que donne Anatolius de l'unité. (§ 1, texte 1).

Texte 4 : Nicomaque de Gérase : crible d'Erathostène, nombres premiers entre eux.

Le chapitre XIII du livre I de l'Introduction arithmétique de Nicomaque nous donne la description du procédé connu encore de nos jours sous le nom de crible d'Erathostène pour l'obtention effective des nombres premiers : on le présente actuellement davantage sous forme de tableau que de ligne. Il nous donne aussi le

moyen de savoir si deux nombres sont, ou non, premiers entre eux à partir du calcul de leur plus grand commun diviseur : on pourra comparer avec le texte d'Euclide qui suivra (algorithme du PGCD) et mesurer la différence de point de vue et donc d'exposition.

NICOMAQUE DE GERASE : Introduction arithmétique.
II siècle après J.C. Livre I, chapitre XIII.
Traduction J. Bertier Vrin 1978.

CHAPITRE XIII

LES NOMBRES IMPAIRS PREMIERS ENTRE EUX. LE CRIBLE D'ERATOSTHENE. LA DETERMINATION DES NOMBRES PREMIERS. LA DETERMINATION DES NOMBRES PREMIERS ENTRE EUX.

2. La genèse de ces nombres est appelée *crible* par Eratosthène, puisque, prenant les *impairs* confondus, indistincts par eux-mêmes, nous les séparons par cette méthode de genèse comme avec un instrument ou un crible, et que nous trouvons à part les nombres *premiers* et *non composés*, à part les nombres *seconds* et *composés*, et séparément les nombres mixtes.

3. Le procédé du *crible* est le suivant : exposant tous les *impairs* successifs à partir de la triade, le plus possible sur une ligne très longue, et partant du premier, j'examine lesquels il peut mesurer, et je trouve qu'il peut mesurer ceux qui en laissent deux entre eux, jusqu'où nous voudrons avancer, et qu'il ne les mesure pas au hasard et n'importe comment, mais qu'il mesurera le premier à se présenter, c'est-à-dire celui qui en laisse deux au milieu, selon la quotité du tout premier disposé dans la ligne, c'est-à-dire selon sa propre quotité (car il le mesure trois fois) ; celui qui en laisse deux en partant de ce nombre, selon la quotité de celui qui est rangé second (car il le mesure cinq fois) ; et plus loin de nouveau, celui qui en laisse deux, selon la quotité de celui qui est rangé troisième (car il le mesure sept fois) et plus loin encore celui qui est disposé au-delà de deux, selon la quotité de celui qui est rangé quatrième (car il le mesure neuf fois), et à l'infini de la même façon.

4. Puis après celui-ci, à partir d'un autre début , je vais au second terme, j'examine lesquels il peut mesurer, et je trouve que ce sont tous ceux qui laissent un intervalle d'une tétrade, mais le premier, selon la quotité du premier terme rangé dans la ligne, car il le mesure trois fois ; le second selon celle du second, car il mesure cinq fois ; le troisième selon celle du troisième, car il le mesure sept fois ; et toujours ainsi en suivant.

5. De nouveau en recommençant, le troisième nombre, le 7, recevant la mesure, mesurera ceux qui laissent un intervalle de six, mais le premier, selon la quotité du 3 rangé premier, le second, selon celle du 5, car ce nombre occupe le second rang, le troisième, selon celle du 7, car ce nombre a le troisième rang dans la ligne.

6. Suivant la même règle, le processus avancera sans entrave pour toi de tout en bout, de sorte que les nombres recevront successivement la *mesure* selon le rang qui leur est réservé dans la ligne, le nombre de termes passés étant réglé selon la croissance bien ordonnée des pairs à partir de la dyade à l'infini, ou selon le doublement du champ selon lequel le nombre qui mesure est rangé, et le *combien* selon la croissance bien ordonnée des impairs à partir de la triade .

7. Si donc tu marques les nombres par des signes, tu trouveras que ceux qui reçoivent la mesure ne mesurent pas tous à la fois le même nombre (parfois il n'y en a même pas deux qui le font) et que tous les nombres exposés ne tombent pas purement et simplement sous l'une de leurs mesures, mais que certains échappent entièrement à la mesure par quelque nombre que ce soit, alors que d'autres sont mesurée par un seul nombre, et d'autres encore par deux ou plus.

8. Ceux donc qui n'ont absolument pas été mesurés, mais fuient la mesure sont *premiers* et *non composés*, séparés en quelque sorte par un *crible*

11. Si on nous fixe deux nombres impairs et que l'on propose et enjoigne de discerner s'ils sont *premiers* entre eux et *non composés* ou *seconds* et *composés* et, s'ils sont *seconds* et *composés*, quel nombre est leur commune mesure, il faut comparer les nombres proposés et retirer toujours le plus petit du plus grand, autant de fois que c'est possible , puis, le plus petit etant retiré, soustraire à son tour du nombre restant, autant de fois encore que cela est possible ; car l'alternance elle-même et la soustraction réciproque cesseront nécessairement soit à l'unité, soit à un unique et même nombre nécessairement *impair*.

12. Lors donc que les soustractions s'achèvent à l'unité, ils montrent que les nombres sont *premiers* et *non composés* entre eux, mais lorsqu'elles vont vers un autre nombre *impair*, qui s'écrit deux fois en quotité , dis que ces nombres sont *seconds* entre eux et *composés* et que leur commune mesure est ce nombre qui s'écrit deux fois ; par exemple, si on nous propose 23 et 45, retire 23 de 45, il restera 22 ; en retirant à son tour ce nombre de 23, le reste est l'unité ; en retirant celle-ci de 22 autant de fois qu'il est possible, tu cesseras à l'unité ; c'est pourquoi ces nombres sont *premiers* et *non composés* entre eux, et leur commune mesure est l'unité qui reste.

13. Mais si on propose d'autres nombres, 21 et 49, retire le plus petit du plus grand : reste 28 ; ensuite, de nouveau je retire de celui-ci le même nombre 21 (car c'est possible), reste 7 ; je retire 7 de 21, reste 14 ; de nouveau j'en retire 7 (car c'est possible), restera 7, mais il n'est pas possible de retirer une hebdomade d'une hebdomade ; la cessation du processus est achevée à 7 qui s'écrit deux fois ; proclame que les nombres initiaux 21 et 49 sont *seconds* et *composés* entre eux, et que leur commune mesure, en plus de l'unité universelle, est 7.

Note : Quotité : nombre d'unités qui définit un nombre ; c'est la mesure du nombre. Exemple la quotité du nombre trois est trois. S'oppose à l'aspect grandeur du nombre, c'est-à-dire le nombre comme mesure. Voici la définition du nombre que donne Nicomaque au chapitre VII : " Le nombre est une multiplicité définie, ou un système d'unités, ou encore un flux de quotité constitué d'unités ".

Remarque. L'ouvrage de Nicomaque de Gérase dont sont extraits ces deux textes, tout en étant un ouvrage d'arithmétique, est aussi une propédeutique à la philosophie, dans la perspective platonicienne (voir généralités). Le titre du chapitre I du livre I est en effet : la philosophie, la sagesse, leur objet.

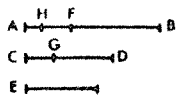
Texte 5 : Euclide : algorithme du PGCD.

Le texte d'Euclide qui suit donne le fameux algorithme du PGCD, souvent appelé algortihme d'Euclide, et dénommé par les grecs anthypharèse c'est-à-dire action d'enlever tour à tour. C'est ce procédé qu'utilise Euclide au livre X pour démontrer que deux grandeurs sont incommensurables (voir Analyse). Cet algorithme se prête tout à fait à la programmation sur une calculatrice de poche. Pour voir son fonctionnement sur des exemples numériques on pourra se reporter au texte précédent de Nicomaque.

EUCLIDE : Eléments, IIIe siècle avant J.C., livre VII.
Traduction : J. Itard. Hermann 1961,

Proposition 1

Deux nombres inégaux étant proposés, le plus petit étant continuellement retranché tour à tour du plus grand, si le nombre qui reste ne mesure jamais celui qui le précède avant qu'il ne reste l'unité, les nombres originaires sont premiers entre eux.



les mesurera. Que quelque nombre les mesure, et que ce soit E; que CD, mesurant BF, laisse FA plus petit que lui. Que FA, mesurant DG, laisse GC plus petit que lui, et que GC, mesurant FH, laisse l'unité AH.

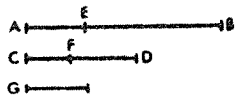
Puisque E mesure CD et que CD mesure BF, E mesure aussi BF. Mais il mesure aussi le tout BA; donc il mesure le reste AF. Mais AF mesure DG; donc E mesure aussi DG. Mais il mesure le tout DC; donc il mesure le reste CG. Mais CG mesure FH; donc E mesure aussi FH. Mais il mesure le tout FA; donc il mesurera le reste, l'unité AH, bien qu'il soit un nombre, ce qui est impossible.

Donc aucun nombre ne mesurera les nombres AB, CD; donc AB, CD sont premiers entre eux. C.Q.F.D.

PROPOSITION 2

Deux nombres non premiers entre eux étant donnés, trouver leur plus grande commune mesure.

Soient AB et CD les deux nombres donnés non premiers entre eux. Il faut trouver la plus grande commune mesure de AB et de CD.



Si CD mesure AB, comme il se mesure lui-même, CD est une commune mesure de CD et de AB. Il est évident qu'il est aussi la plus grande; car aucun nombre plus grand que CD ne peut mesurer CD.

Mais si CD ne mesure pas AB, et si le plus petit des nombres AB, CD est continuellement soustrait du plus grand, il restera quelque nombre qui mesurera celui qui est avant lui.

Car il ne restera pas l'unité, sans quoi AB, CD seraient premiers entre eux, ce qui est contraire à l'hypothèse, Il restera donc quelques nombre qui mesurera celui qui est avant lui.

Que CD, mesurant BE, laisse EA plus petit que lui-même; que EA, mesurant FD, laisse FC plus petit que lui-même, et que CF mesure AE.

Puisque CF mesure AE et que AE mesure DF, CF mesure aussi DF. Mais il se mesure lui-même; il mesure donc le tout CD.

Mais CD mesure BE; donc CF mesure aussi BE. Mais il mesure EA. Il mesure donc le tout BA. Mais il mesure CD. Donc CF mesure AB, CD. Ainsi CF est une commune mesure de AB, CD.

Je dis de plus qu'il est aussi la plus grande.

Car, si CF n'est pas la plus grande mesure de AB, CD, quelque nombre plus grand que CF mesurera les nombres AB, CD.

Qu'un tel nombre les mesure, et que ce soit G. Puisque G mesure CD et que CD mesure BE, G mesure aussi BE. Mais il mesure le tout BA; il mesure donc aussi le reste AE. Mais AE mesure DF, donc G mesurera aussi DF. Mais il mesure le tout DC. Il mesurera donc le reste CF, le plus grand le plus petit, ce qui est impossible.

Donc aucun nombre plus grand que CF ne mesurera les nombres AB, CD; donc CF est la plus grande commune mesure de AB, CD.

Porisme

Il suit évidemment de là, que si un nombre en mesure deux autres, il mesure aussi leur plus grande commune mesure. C.Q.F.D.

Texte 6 : Euclide : un exemple de démonstration par descente infinie et la décomposition d'un nombre en facteurs premiers.

Egalement tirée de Eléments d'Euclide la proposition 31 montre un bel exemple d'une technique arithmétique de démonstration qu'utilisera beaucoup Fermat (voir §5 texte 11 et §7 texte 20) et bien des mathématiciens à sa suite pour résoudre des problèmes arihtmétiques : la descente infinie. De plus c'est ce théorème qui assure la décomposition d'un nombres entier en facteurs premiers.

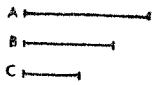
EUCLIDE : Eléments, IIIe siècle avant J.C., livre VII.
Traduction : J. Itard. Hermann 1961,

PROPOSITION 31

Tout nombre composé est mesuré par quelque nombre premier.

Que A soit un nombre composé. Je dis que A est mesuré par quelque nombre premier.

Car, puisque A est composé, quelque nombre le mesurera. Qu'un nombre le mesure et que ce soit B. Si B est premier on aura ce qui est proposé. Mais s'il est composé quelque nombre le mesurera.



Qu'un nombre le mesure et que ce soit C. Comme C mesure B et que B mesure A, C mesure aussi A. Si C est premier on aura ce qui est proposé. Mais s'il est composé quelque nombre le mesurera.

Si la recherche est continuée ainsi on trouvera quelque nombre premier qui mesurera. Car si l'on ne trouvait pas un nombre premier, il y aurait une infinité de nombres qui mesureraient A, et qui seraient plus petits les uns que les autres, ce qui est impossible dans les nombres. On trouvera donc quelque nombre premier qui mesurera celui qui est avant lui, et qui mesurera A. Donc tout nombre composé est mesuré par quelque nombre premier. C.Q.F.D.

PROPOSITION 32

Tout nombre est premier, ou est mesuré par quelque nombre premier.

Soit le nombre A. Je dis que A est premier ou est mesuré par quelque nombre premier.

Si A est premier, on aura ce qui est proposé. S'il est composé quelque nombre premier le mesurera, donc tout nombre est premier ou est mesuré par quelque nombre premier. C.Q.F.D.

Texte 7 : Euclide : l'ensemble des nombres premiers est infini.

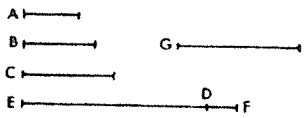
EUCLIDE : Eléments, IIIe siècle après J.C., livre IX.
Traduction : J. Itard. Hermann 1961.

PROPOSITION 20

Les nombres premiers sont plus nombreux que toute multitude proposée de nombres premiers.

Soient A, B, C les nombres premiers que l'on aura proposés. Je dis que les nombres premiers sont plus nombreux que A, B, C.

Car soit pris le plus petit nombre mesuré par A, B, C et que ce soit DE. Ajoutons l'unité DF à DE. EF sera premier ou non.



Qu'il soit d'abord premier. On aura trouvé les nombres premiers A, B, C, EF, plus nombreux que les nombres A, B, C.

Mais que EF ne soit pas premier. Il est mesuré par quelque nombre premier. Qu'il soit mesuré par le nombre premier G. Je dis que G n'est aucun des nombres A, B, C. Car, si possible, qu'il en soit un. A, B, C mesurent DE, donc G mesurera aussi DE. Mais il mesure encore EF. Donc G, qui est un nombre, mesurera le reste, l'unité EF, ce qui est absurde.

Donc G n'est aucun des nombres A, B, C et il est premier par hypothèse.

On a donc trouvé les nombres premiers A, B, C, G, plus nombreux que la multitude proposée A, B, C. C.Q.F.D.

3 - NUMERATION.

La trop grande familiarité que nous avons avec notre écriture des nombres nous fait perdre de vue le rôle que joue la base de numération dans les questions arithmétiques. Si les nombres décimaux, grâce à l'extension du principe de numération de position aux puissances négatives de 10, sont inventés et utilisés par quelques mathématiciens isolés (Bonfils de Tarascon au XIVe siècle et Al Kashi au XVe siècle) ce n'est qu'à la fin du XVIe siècle que Viète et surtout Stevin essaient d'en imposer l'usage ; dans le texte de Stevin proposé on pourra apprécier sa verve et son talent pour faire adopter son invention et pour proposer la division décimale des unités de mesure. Mais il faudra, en France, attendre la Révolution pour voir la Convention adopter en 1795 le calcul décimal et le système métrique, celui-ci devenant obligatoire en 1837. D'autre part nous avons peut-être oublié certaines propriétés des nombres dépendent de la base de numération : ainsi en est-il des caractères de divisibilité dont nous parle Pascal dans le deuxième texte. Enfin si la base dix l'a finalement emporté, il n'en demeure pas moins que d'autres bases sont utilisées, en particulier en informatique, la base seize (système hexadécimal) et la base deux (système binaire). C'est à ce dernier que Leibniz consacre l'article reproduit ici.

Texte 8 : Stevin : les nombres décimaux.

L'extrait de la Disme de Stevin présenté ici est en fait le début d'un ouvrage très bref (8 pages) publié pour la première fois en flamand en 1585 et traduit en français la même année. Il donne ensuite, de façon analogue à l'addition, la technique de la soustraction, de la multiplication et de la division. Le livret se termine par un appendice expliquant comment appliquer concrétement les calculs dans six métiers recouvrant " tous comptes se rencontrant aux affaires des hommes ". Le succés de cet opuscule, adressé aux utilisateurs, a été considéble.

STEVIN : Disme, 1585.
Adaptation de la traduction française de A. Girard 1634, pages 1, 2, 3.

THIENDE

Leerende door onghehoorde lichticheyt allen rekeningen onder den Menſchen noodich vallende, afveerdighen door heele ghetalen ſonder ghebrokenen.

Beſchreven door SIMON STEVIN *van Brugghe.*

TOT LEYDEN,
By Chriſtoffel Plantijn.
M. D. LXXXV.

L A D I S M E

Qui enseigne à expédier facilement avec des nombres entiers, sans fractions (1), tous les comptes qui se rencontrent dans les affaires des hommes.

D'abord écrite en Flamand, et maintenant traduite en Français, par Simon STEVIN de Bruges.

Aux Astrologues, Arpenteurs , Mesureurs de tapisserie, Jaugeurs, Stéréométriens en général (2), Maîtres de monnaie, et à tous les Marchands,

SIMON STEVIN Salut.

Quelqu'un voyant la petitesse de ce livret, et la comparant à votre grandeur, mes très honorés Seigneurs, auxquels il est dédié, estimera peut-être absurde ce que nous avons conçu. Mais s'il considére la proportion qu'il y a entre, d'une part le petit volume de ce livret et l'humaine faiblesse de ses destinataires, et d'autre part sa grande utilité et leur esprit profond et ingénieux (3), il se rendra compte qu'il a comparé des termes extrêmes, qui ne permettent pas de convertir cette comparaison en une proportion. Considérons donc le rapport du troisième terme au quatrième. Mais que va-t-on proposer ? D'aventure quelque invention admirable ? Non certes, mais une chose si simple qu'elle ne mérite quasiment pas le nom d'invention, car comme l'homme rustique et lourd trouve bien d'aventure quelque grand trésor, sans avoir pour cela usé de science, c'est ainsi quelque chose de semblable qui est arrivé en cette affaire. Pourtant si quelqu'un juge que je me vante de mon esprit à cause de l'explication que je donne de son utilité, sans aucun doute il démontre, ou qu'il n'y a en lui ni jugement, ni intelligence, pour savoir discerner les choses simples des ingénieuses, ou qu'il est jaloux de ce qui contribue à la prospérité commune ; mais quoiqu'il en soit, il ne faut pas omettre l'utilité de celui-ci, pour l'inutile calomnie de celui-là. Or comme le marinier, qui a d'aventure trouvé quelque île inconnue, déclare franchement au Roi toutes ses richesses, comme d'avoir de beaux fruits, de précieux minéraux, de plaisantes contrées, etc, sans que cela passe pour de l'orgueil, de même nous parlerons ici librement de la grande utilité de cette invention, je dis grande, voire plus grande qu'aucun de vous autres ne s'y attend, sans toutefois m'en glorifier.

Vu donc que la matière de cette DISME (dont le nom sera justifié par la première définition qui suivra) est le nombre, et que son utilité vous est, Messieurs, bien connue par vos expériences continuelles, il ne sera point

besoin d'en parler longuement. Car si quelqu'un est Astrologue, il sait que le monde est devenu grâce aux calculs astronomiques (car ils enseignent au pilote l'élévation de l'équateur et du pôle, au moyen de la table des déclinaisons du soleil, on décrit avec celle-ci la vraie longitude et latitude des lieux, etc...) un paradis, abondant en plusieurs lieux de ce que toutefois la terre n'y peut point produire. Mais comme le doux n'est jamais sans l'amer, le travail occasionné par de tels calculs lui est connu, à cause des laborieuses multiplications et divisions qui découlent de la progression par soixantièmes des degrés, minutes, secondes, tierces, etc... Mais s'il est Arpenteur, il sait le grand bénéfice que le monde reçoit de sa science, par laquelle s'évitent plusieurs difficultés et querelles, qui surviendraient journellement, par ignorance de la surperficie des terres ; outre cela il n'ignore pas (principalement celui qui a de grandes affaires) les ennuyeuses multiplications qui découlent des verges, pieds et souvent doigts (4), multipliés l'une par l'autre, ce qui n'est pas seulement importun, mais (même si les mesures et autres choses précédentes étaient bien exécutées) est souvent cause d'erreur, tendant à causer un grand dommage à l'un ou l'autre, ainsi que la ruine de la renommée de l'Arpenteur. Et de même des Maîtres de monnaies, Marchands, et autres métiers. Mais d'autant plus importants sont ceux-là, et les voies pour y parvenir plus laborieuses, d'autant plus grande est cette découverte de la DISME qui ôte toutes ces difficultés. Mais comment ? Elle enseigne (afin de dire beaucoup en un mot) à expédier facilement sans nombres fractionnaires tous les comptes qui se rencontrent dans les affaires humaines ; de sorte que les quatre principes d'Arithmétique que l'on appelle ajouter, soustraire, multiplier et diviser avec des nombres entiers, pourront rendre un tel service, procurant la même facilité à ceux qui usent de jetons. Or si par un tel moyen sera sauvé ce qui se perdrait autrement, si par un tel moyen sera ôté labeur, querelle, erreur, dommage, et autres accidents communément associés à ceux-ci, je le soumets volontiers à votre jugement.

Quant à ce que quelqu'un pourrait me dire, que beaucoup d'inventions semblent bonnes au premier regard, mais quand on veut s'en servir, on ne peut rien en faire, comme il arrive souvent aux chercheurs de grandes inspirations, qui semblent bonnes dans les petites épreuves, mais qui dans les grandes, ou à l'usage, ne valent rien, nous lui répondrons qu'il n'y a ici un tel doute, parce que l'on en fait journellement l'expérience de façon concrète ; à savoir par divers Arpenteurs Hollandais experts, auxquels nous l'avons soumise, lesquels (laissant ce qu'ils avaient inventé chacun à sa manière, pour amoindrir le travail de leurs calculs) l'utilisent à leur grande satisfaction et avec le fruit qui, par nature, doit nécessairement

s'en suivre. La même chose chose arrivera à chacun de vous autres, mes Très honorés Seigneurs, qui fera comme eux. Vivez cependant en toute félicité.

ARGUMENT

La DISME a deux parties : définitions et opérations. Dans la première partie on dira par la première définition, ce qu'est la DISME ; par la seconde, troisième et quatrième, ce que signifie commencement, prime, seconde, etc et nombres de DISME. Dans l'opération on dira par quatre propositions, l'addition, soustraction, multiplication et division des nombres de DISME, dont la structure peut se représenter succintement par cette table :

- *La Disme a deux parties*
  - *définition de ce qu'est :*
    - *Disme*
    - *Commencement*
    - *Prime, seconde, etc*
    - *Nombre de Disme*
  - *Opération de :*
    - *L'addition*
    - *Soustraction*
    - *Multiplication*
    - *Division.*

A la fin on trouvera encore un Appendice, disant l'usage de la Disme par quelques exemples concrets.

LA PREMIERE PARTIE DE LA DISME

Des définitions

- DEFINITION I -

Disme est une espèce d'Arithmétique, inventée par la progression en dixième, ayant pour caractères des chiffres, par lesquels se décrivent tout nombre, et par laquelle l'on expédie avec des nombres entiers sans fractions, tous les comptes qui se rencontrent dans les affaires des hommes.

EXPLICATION

Soit un nombre : mille cent onze, écrit avec les caractères des chiffres de cette façon 1111, pour lesquels il apparait que chaque 1 est la dixième partie du caractère précédent le plus proche. Pareillement pour 2378 : chaque unité du 8 est la dixième de chaque unité du 7. Et de même de tous les autres. Mais parce qu'il est convenable que les choses dont on veut parler aient des noms et que ce type de calcul est obtenu par la considération

d'une telle progression par dixième ou disme, voire qu'elle consiste entièrement en elle, comme il apparaitra dans ce qui suit, nous nommons ce traité proprement et convenablement la DISME ; par là même on peut opérer avec des nombres entiers sans fractions dans tous les comptes se rencontrant dans nos affaires, comme on le démontre par la suite.

- DEFINITION II -

Tout nombre entier proposé s'appelle COMMENCEMENT, son signe est ⓪.

EXPLICATION

Par exemple soit un nombre quelconque : trois cent soixante quatre ; nous le nommons trois cent soixante quatre COMMENCEMENTS, le décrivant ainsi : 364 ⓪ . Et ainsi pour tous les autres.

- DEFINITION III -

Et chaque dixième partie de l'unité du commencement nous la nommons PRIME, son signe est ①; et chaque dixième partie de l'unité de prime nous la nommons SECONDE, son signe est ② . Et ainsi pour chaque dixième partie de l'unité de son signe précédent, toujours d'ordre un de plus.

EXPLICATION

Comme 3 ① 7 ② 5 ③ 9 ④ c'est-à-dire 3 primes 7 secondes 5 tierces 9 quartes ; et ainsi on pourrait continuer à l'infini. Mais pour dire leur valeur il est évident que les dits nombres font $\frac{3}{10}$ $\frac{7}{100}$ $\frac{5}{1000}$ $\frac{9}{10000}$, *soit ensemble* $\frac{3759}{10000}$. *Pareillement 8 ⓪ 9 ① 3 ② 7 ③ valent 8* $\frac{9}{10}$ $\frac{3}{100}$ $\frac{7}{1000}$, *soit ensemble* $8\frac{937}{1000}$. *Et ainsi pour les autres. Il faut savoir aussi que nous n'utilisons dans la DISME aucun nombre fractionnaire, et que le nombre placé devant les signes excepté ⓪ , n'excède jamais le 9. Par exemple nous n'écrivons pas 7 ① 12 ② mais à la place 8 ① 2 ② car ils valent autant.*

- DEFINITION IV -

Les nombres de la précédente et troisième définition s'appellent en général NOMBRES DE DISME.

Fin des Définitions.

SECONDE PARTIE DE LA DISME

DE L'OPERATION

- PROPOSITION I, DE L'ADDITION -

Etant donnés des nombres de Disme à ajouter : trouver leur somme.

Explication de ce qui est donné. Soit trois nombres de Disme, lesquels sont le premier $27\,⓪\,8\,①\,4\,②\,7\,③$, *le deuxième* $37\,⓪\,6\,①\,7\,②\,5\,③$, *le troisième* $875\,⓪\,7\,①\,8\,②\,2\,③$.

Explication de ce qui est demandé. Il nous faut trouver la somme. Construction. On mettra les nombres donnés en les joignant ainsi, les ajoutant selon la méthode usuelle pour ajouter les nombres entiers, de cette manière :

⓪	①	②	③
27	8	4	7
37	6	7	5
875	7	8	2
941	3	0	4

Ce qui nous donne pour somme (par le problème 1 de l'Arithmétique) 941304, qui est (ce que démontrent les signes au dessus des nombres) $941\,⓪\,3\,①\,0\,②\,4\,③$.

Je dis que les nombres donnés font la somme cherchée. Démonstration. Les $27\,⓪\,8\,①\,4\,②\,7\,③$ *donnés, font (par la 3° définition)* $27\ \frac{8}{10}\ ,\ \frac{4}{100}\ ,\ \frac{7}{1000}$, *ensemble* $27\ \frac{847}{1000}$, *et pour la même raison* $37\,⓪\,6\,①\,7\,②\,5\,③$ *vaut* $37\ \frac{675}{1000}$, *et* $875\,⓪\,7\,①\,8\,②\,4\,③$ *fera* $875\ \frac{782}{1000}$, *ces trois nombres, soit* $27\ \frac{847}{1000}$, $37\ \frac{675}{1000}$, $875\ \frac{782}{1000}$, *font ensemble (par le 10e problème de l'Arithmétique)* $941\ \frac{304}{1000}$, *mais la somme* $941\,⓪\,3\,①\,0\,②\,4\,③$ *vaut autant, c'est donc la vraie somme, ce qu'il fallait faire.*

NOTA

Si aux nombres donnés manque quelque signe de leur ordre naturel, on le remplacera par celui manquant. Soient par exemple les nombres donnés $8\,⓪\,5\,①\,6\,②$ *et* $5\,⓪\,7\,②$, *auquel manque, pour le dernier, le signe de l'ordre* ①. *On mettra à sa place* $0\,①$, *prenant alors pour nombre donné* $5\,⓪\,0\,①\,7\,②$, *les ajoutant comme ci-dessous de cette manière :*

⓪	①	②
8	5	6
5	0	7
1	3	6	3

Cet avertissement servira aussi aux trois propositions suivantes, là où il faut toujours remplir l'ordre des figures manquantes, comme nous l'avons fait sur cet exemple .....

NOTES :

1 - *Dans le texte : rompus.*
Rompu voulait dire fractionnaire.

2 - *Les jaugeurs étaient ceux qui mesuraient les volumes des tonneaux.*
Les stéréométriens mesuraient plus généralement les volumes.

3 - *La proportion dont il est question est l'égalité des deux rapports suivant :*

$$\frac{\text{petit volume}}{\text{humaine faiblesse}} = \frac{\text{grande utilité}}{\text{esprit profond et ingénieux}}$$

qui font intervenir quatre termes comme toute proportion :

$$\frac{a}{b} = \frac{c}{d}$$

c et d sont les troisièmes et quatrièmes termes de la proportion.

4 - *Anciennes unités de longueur.*

LA DISME,

Enſeignant facilement expedier par nombres entiers ſans rompuz, tous comptes ſe rencontrans aux affaires des Hommes.

Premierement deſcripte en Flameng, & maintenant convertie en Francoïs, par SIMON STEVIN *de Bruges.*

AVX ASTROLOGVES, ARPENTEURS, MESVREVRS DE TAPISSERIE, GAVIEVRS, STEREOMETRIENS EN general, Maiſtres de monnoye, & à tous Marchans:

SIMON STEVIN *Salut.*

QVelcun voyant la petiteſſe de ce livret, & la comparant à la grandeur de vous mes Tres-honnorez Seigneurs ; auſquels il eſt dedié, eſtimera peut eſtre noſtre concept abſurd ; Mais s'il conſidere la Proportion, qui eſt, comme la petite quantité de ceſtui cy, à l'humaine imbecillité de ceux la, ainſi ſes grandes utilitez, à leurs hauts & ingenieux entendemens, ſe trouvera avoir faict comparaiſon des termes extremes, leſquels ne la permettent en converſion de proportion quelconque. Soit doncques le troiſieſme au quatrieſme. Mais que ſera ce proposé? d'aventure quelque invention admirable? non certes, mais choſe ſi ſimple qu'elle ne merite quaſi le nom d'invention, car comme l'homme ruſtique, & lourd, trouve bien d'aventure quelque grand treſor, ſans y avoir uſé de ſcience, tout ainſi le ſemblable eſt il advenu en ceſt affaire: Pourtant ſi quelcun me vouluſt eſtimer pour vanteur de mon entendement à cauſe de l'explication de ces vtilitez ; ſans doubte il demonſtre, ou qu'il n'y a en luy luy ny jugement, ny intelligence, de ſçavoir diſcerner les choſes ſimples des ingenieuſes, ou qu'il ſoit envieux de la proſperité commune ; mais quoy qu'il en ſoit, il ne faut pas omettre l'utilité de ceſtui cy, pour l'inutile calomnie de ceſtuy la. Or comme le marinier ayant d'aventure trouvé quelque Iſle incognue, declare franchement au Roy toutes ſes richeſſes, comme d'avoir beaux fruicts, precieux mineraux, plaiſantes contrees, &c. ſans que cela luy ſoit reputé pour philautie, ainſi nous parlerons icy librement de la Grande utilité de ceſte invention, je di Grande, voire plus Grãde que je n'eſtime qu'aucun de vous autres attende, ſans toutesfois me glorifier du mien.

Veu doncques que la matiere de ceſte DISME *(la cauſe duquel nom ſera declarée par la ſuyvante premiere definition) eſt nombre, l'utilité des effects de laquelle, vous Mrs eſt aſſés notoire par vos continuelles experiences, il ne ſera point meſtier d'en faire beaucoup de parolles ; Car s'il eſt Aſtrologue, il ſçait que le monde eſt devenu par les computations Aſtronomiques (car elles enſeignent au Pilote l'elevation de l'Equateur, & du Pole, par le moyen de la table des declinations du Soleil, l'on deſcript par icelles la vraye longitude & latitude des lieux, &c.) vn paradis, abondant en pluſieurs lieux, de ce que toutesfois la terre n'y peut point produire. Mais comme le*

Texte 9 : Pascal : les caractères de divisibilité.

Cet écrit de Pascal se propose de justifier les règles connues de divisibilité par 9, 3, etc..., et de les généraliser. Pascal met en évidence, à la fin, la façon dont elles dépendent de la base dix, et donc montre comment on peut utiliser la méthode décrite pour obtenir des caractères de divisibilité dans une base quelconque. On pourra comparer la méthode de Pascal avec celle donnée par Gauss à la fin du texte sur les congruences figurant au § 5, texte 13.

PASCAL : Des caractères de divisibilité des nombres déduits de la somme de leurs chiffres vers 1654.

Pages 84 à 89. Oeuvres complètes, Seuil 1963.

DES CARACTÈRES DE DIVISIBILITÉ DES NOMBRES DÉDUITS DE LA SOMME DE LEURS CHIFFRES

REMARQUE PRELIMINAIRE

Rien de plus connu en arithmétique que la proposition d'après laquelle un multiple quelconque de 9 se compose de chiffres dont la somme est elle-même un multiple de 9. Si, par exemple, on additionne les chiffres dont se compose 18, double de 9, on trouve 1 + 8 = 9. De même, en additionnant les chiffres d'un nombre quelconque, on reconnaîtra si ce nombre est divisible par 9. Ainsi 1719 est un multiple de 9, parce que la somme 1 + 7 + 1 + 9 ou 18 de tous ses chiffres est elle-même divisible par 9. Bien que cette règle soit communément employée, je ne crois pas que personne jusqu'à présent en ait donné une démonstration ni ait cherché à en généraliser le principe. Dans ce petit traité, je justifierai le caractère de divisibilité par 9 et plusieurs autres analogues; j'exposerai aussi une méthode générale qui permet de reconnaître, à la simple inspection de la somme de ses chiffres, si un nombre donné est divisible par un autre nombre quelconque; cette méthode ne s'applique pas seulement à notre système décimal de numération (système qui repose sur une convention, d'ailleurs assez malheureuse, et non sur une nécessité naturelle, comme le pense le vulgaire), mais elle s'applique encore sans défaut à tout système de numération ayant pour base tel nombre qu'on voudra, ainsi qu'on le verra dans les pages qui suivent.

PROPOSITION UNIQUE

Reconnaître, à la seule inspection de la somme de ses chiffres, si un nombre donné est divisible par un autre nombre donné.

Pour plus de généralité nous remplacerons les nombres par des lettres. Soit donc un diviseur quelconque que nous représenterons par la lettre A, et soit un dividende TVNM dans lequel les lettres M, N, V, T représentent respectivement les chiffres des unités simples, des dizaines, des centaines, des unités de mille, et ainsi de suite : de telle sorte que, pour passer des quantités littérales aux quantités numériques, il suffirait de remplacer chacune des lettres par l'un des 9 premiers nombres, par exemple M par 4, N par 3, V par 5, T par 6, ce qui donnerait pour dividende 6534, le diviseur A étant un nombre quelconque tel que 7. Mais nous laisserons de côté les exemples particuliers afin de comprendre tous les cas possibles dans une même solution générale. Etant donné donc le dividende TVNM et un diviseur quelconque A, il s'agit de reconnaître, à la seule inspection de la somme de ses chiffres, si ce dividende est exactement divisible par A.

Écrivons sur une même ligne, et dans l'ordre décroissant, les nombres de la suite naturelle, puis au dessous, une autre suite de nombres, de manière à former le tableau :

10	9	8	7	6	5	4	3	2	1
K	I	H	G	F	E	D	C	B	1

Dans ce tableau, les nombres de la seconde ligne sont formés comme il suit :

Au-dessous de l'unité on place l'unité.

De celle-ci prise *dix fois*, c'est-à-dire du nombre 10, on retranche le diviseur A autant de fois que possible, et l'on écrit le reste B sous le nombre 2.

De B pris *dix fois* on retranche de même le diviseur A autant de fois que possible, et l'on écrit le reste C sous le nombre 3.

De 10 C on retranche encore le diviseur A autant de fois que possible, et l'on écrit le nouveau reste D sous le nombre 4.

Et ainsi de suite.

Prenons maintenant le dernier chiffre du dividende, M, qui est le premier à partir de la droite, et multiplions-le par l'unité (qui dans notre tableau se trouve placé sous le chiffre 1).

Prenons ensuite le second chiffre, N, et multiplions-le par le nombre B, qui dans notre tableau se trouve placé sous le chiffre 2; puis écrivons le produit au-dessous de M.

Prenons encore le troisième chiffre V, multiplions-le par C (nombre placé sous le chiffre 3), et écrivons le produit sous les produits précédents.

M
N × B
V × C
T × D

Opérons de même pour T, et ainsi de suite.

Je dis que, pour que le nombre proposé TVNM soit divisible par A, il faut et il suffit que la somme M + N × B + V × C + T × D, etc., soit elle-même divisible par A.

Il est évident que si le nombre proposé n'a qu'un seul chiffre M, M est divisible par A, car le nombre tout entier se réduit à M.

Soit maintenant un nombre de *deux* chiffres, représenté par NM; je dis que, pour qu'il soit divisible par A, il faut et il suffit que la somme M + N × B le soit.

En effet, le chiffre N, placé dans la colonne des dizaines, équivaut à 10 N.

Or, d'après le calcul, 10—B est un multiple de A.

Multipliant par N, 10 N—B × N sera aussi un multiple de A.

Si donc il arrive que M + B × N soit un multiple de A.

La somme de ces deux dernières quantités, savoir 10 N + M, sera elle-même un multiple de A.

Donc 10 N + M, c'est-à-dire le nombre proposé NM est un multiple de A. C.q.f.d.

Soit encore un nombre de *trois* chiffres VNM. Pour qu'il soit divisible par A, je dis qu'il faut et suffit que la somme M + N × B + V × C soit elle-même divisible par A.

En effet, le chiffre V, placé dans la colonne des centaines, équivaut à 100 V.

Or, d'après le calcul, 10—B est un multiple de A;

Multipliant 10—B par 10, 100—10 B sera aussi un multiple de A:

Multipliant encore par V, 100 V—10 B × V sera multiple de A;

Mais d'après le calcul, 10 B—C est un multiple de A:

Multipliant par V, 10 B × V—C × V sera multiple de A;

Et, comme on vient d'établir que 100 V—10 B × V est un multiple de A,

la somme de ces deux dernières quantités, savoir 100 V —C × V, sera elle-même un multiple de A;

Mais nous montrerons comme dans le second cas que 10 N—B × N est un multiple de A;

Donc la somme des deux dernières quantités, savoir 100 V + 10 N—C × V—B × N, sera un multiple de A;

Si donc il arrive que C × V + N × B + M soit un multiple de A; la somme des deux dernières quantites écrites, savoir 100 V + 10 N + M, sera encore un multiple de A;

Mais 100 V + 10 N + M, c'est le nombre proposé VNM; donc ce nombre est un multiple de A. C.q.f.d.

La démonstration serait la même si le nombre donné se composait de plus de trois chiffres.

Exemples

Soit à chercher quels sont les multiples du nombre 7. J'écris la suite des dix premiers nombres, et je forme le tableau

10	9	8	7	6	5	4	3	2	1
6	2	3	1	5	4	6	2	3	1

en procédant comme il suit :

J'écris l'unité sous l'unité.

De l'unité, prise 10 fois, je retranche 7 autant de fois que possible, et je place le reste 3 sous le chiffre 2.

Je multiplie le reste 3, par 10 et du produit 30 je retranche 7 autant de fois que possible; je place le nouveau reste 2 sous le chiffre 3.

De 20 je retranche 7 autant de fois que possible; il reste 6 que j'écris sous 4.

De 60 je retranche 7 autant de fois que possible; il reste 4 que j'écris sous 5.

De 40 je retranche 7 autant de fois que possible; il reste 5 que j'écris sous 6.

De 50 je retranche 7 autant de fois que possible; il reste 1 que j'écris sous 7.

De 10 je retranche 7 autant de fois que possible, ce qui me fait retomber sur le premier reste obtenu, savoir 3, que j'écris sous 8.

De 30 je retranche 7 autant de fois que possible: je retrouve le second reste obtenu, savoir 2, que j'écris sous 9.

Les restes déjà obtenus, savoir 1, 3, 2, 6, 4, 5, se retrouvent donc dans le même ordre, et ainsi indéfiniment.

Soit alors à reconnaître si un nombre quelconque 287 542 178 est un multiple de 7.

Je prends le premier chiffre du nombre à partir de la droite, et je le multiplie par l'unité (qui dans notre tableau est placée sous le nombre 1). J'écris donc le produit de 8 par l'unité, c'est-à-dire 8

J'écris ensuite le produit de 7 par le chiffre 3 placé sous 2 dans notre tableau, soit 21

Puis le produit de 1 par 2 2

le produit de 2 par 6 12

le produit de 4 par 4 16

le produit de 5 par 5 25

le produit de 7 par 1 7

le produit de 8 par 3 24

le produit de 2 par 2 4

et je fais la somme 119

Si 119 est divisible par 7, le nombre proposé 287 542 178 le sera aussi.

La même méthode peut encore servir à reconnaître si 119 est un multiple de 7.

On multipliera 9 par l'unité, ce qui donne 9

Puis 1 par 3 3

Et enfin 1 par 2 2

Et l'on fera la somme 14

Si cette somme est divisible par 7, 119 le sera également.

Enfin, et par curiosité plutôt que par nécessité, on pourra traiter encore le nombre 14 comme on a traité 119, c'est-à-dire :

Multiplier 4 par l'unité, ce qui donne. 4

Puis 1 par 3. 3

Et faire la somme. 7

Celle-ci étant évidemment divisible par 7, le nombre 14 le sera aussi, partant 119 le sera, et par suite, enfin, le nombre proposé 287 542 178 sera lui-même un multiple de 7.

Soit à chercher quels sont les nombres divisibles par 6.

Les nombres naturels étant encore écrits les uns à côté des autres, je forme le tableau

4	3	2	1
4	4	4	1

en procédant comme il suit :

Je pose l'unité sous l'unité; je retranche 6 de 10, et je place le reste 4 sous 2; je retranche ensuite 6 de 40 autant de fois que possible, et je place le reste 4 sous 3; et ainsi de suite : le reste 4 se reproduira indéfiniment.

Soit alors à chercher si un nombre donné quelconque, 248 742, est divisible par 6.

J'écris le dernier chiffre du nombre. 2

puis le chiffre précédent multiplié par 4. 16

puis le chiffre précédent multiplié par 4, etc.. . . 28

puis. 32

. 16

. 8

102

Si la somme 102 est divisible par 6, le nombre 248 742 sera lui-même divisible par 6.

Un nombre quelconque étant donné, reconnaître s'il est divisible par 3.

On construira, comme dans les exemples précédents, le tableau :

5	4	3	2	1
1	1	1	1	1

Pour cela, on pose l'unité sous l'unité; on retranche 3 de 10 autant de fois que possible et on place le reste 1 sous 2; puis on retranche 3 de 10 autant de fois que possible et on place le reste 1 sous 3; et ainsi de suite indéfiniment.

Soit alors à reconnaître si un nombre donné quelconque 2 451, est divisible par 3. J'écris

le dernier chiffre 1

le précédent 5

puis. 4

. 2

12

Si la somme 12 est divisible par 3, il en sera de même du nombre proposé.

Un nombre étant donné, reconnaître s'il est divisible par 9.

Ici encore, si on forme le tableau obtenu en plaçant l'unité sous l'unité, retranchant 9 de 10, etc., on voit que le reste 1 se répète indéfiniment. Donc, pour qu'un nombre quelconque soit divisible par 9, il suffit que la somme de ses chiffres le soit.

Un nombre étant donné, reconnaître s'il est divisible par 4.

Comme dans les exemples précédents, on forme le tableau :

4	3	2	1
0	0	2	1

Pour cela, on pose l'unité sous l'unité; on retranche 4 de 10 autant de fois que possible et on place le reste 2 sous 2; de 20 on retranche 4 autant de fois que possible, et on place le reste 0 sous 3; de 0 on retranche 4 : il reste toujours 0.

Soit alors donné le nombre 2 486. J'écris

le dernier chiffre 6

le précédent multiplié par 2. 16

22

Le chiffre précédent multiplié par 0 donne 0; et ainsi de suite. La condition nécessaire et suffisante pour que le nombre donné soit divisible par 4 est donc que la somme 22 le soit.

On trouvera de même que, pour qu'un nombre soit divisible par 8, il faut et il suffit que la somme formée du chiffre des unités, du double de celui des dizaines et du quadruple de celui des centaines (les autres chiffres étant négligés comme donnant 0), soit un multiple de 8.

Prenons un dernier exemple.

Soit à chercher quels sont les nombres divisibles par 16.

Les nombres naturels 1, 2, 3, 4, ... étant écrits, je forme le tableau

7	6	5	4	3	2	1
0	0	0	8	4	10	1

en procédant comme il suit :

J'écris l'unité sous l'unité. De 10 je retranche 16 autant de fois que possible : il reste 10 (en effet d'un nombre donné on ne peut pas retrancher un nombre plus grand); j'écrirai donc sous 2 le nombre 10 lui-même. De 10 pris 10 fois suivant la règle habituelle, c'est-à-dire de 100, je retranche 16 autant de fois que possible : il reste 4 que je pose sous 3. De 40 je retranche 16 autant de fois que possible : je pose le reste 8 sous 4. De 80 je retranche 16 autant de fois que possible : il reste 0.

Donc, pour qu'un nombre soit divisible par 16, il faut et il suffit qu'en ajoutant ensemble le chiffre des unités, 10 fois celui des dizaines, 4 fois celui des centaines et 8 fois celui des unités de mille, la somme obtenue soit elle-même divisible par 16.

On reconnaîtra de même que tous les nombres pour lesquels le décuple de l'avant-dernier chiffre, ajouté à tous les autres chiffres (chiffre des unités, chiffre des centaines, etc.), pris une fois chacun, donne une somme divisible par 45, 18, 15, 30, ou 90, c'est-à-dire par l'un des diviseurs à deux chiffres de 90, seront eux-mêmes des multiples de ce diviseur.

Il serait facile d'étendre encore ces exemples : mais il suffit d'avoir ouvert la route et éclairé par une démonstration précise ce sujet nouveau et assez obscur. Les caractères de divisibilité des nombres déduits de la somme de leurs chiffres reposent à la fois sur la nature intime des nombres et sur leur représentation dans le système de numération décimale. Dans tout autre système, par exemple dans le système duodécimal (système fort commode sans doute) qui, outre les neuf premiers chiffres, emploie deux figures nouvelles pour désigner, l'une le nombre 10, l'autre le nombre 11, dans ce mode de numération, il ne serait plus vrai que tout nombre dont la somme des chiffres est un multiple de 9 est lui-même divisible par 9.

Mais la méthode que j'ai fait connaître et la démonstration que j'en ai donnée, conviennent encore à ce système ainsi qu'à tout autre.

Veut-on, dans le système duodécimal, reconnaître si un nombre est divisible par 9, on écrit, comme on l'a fait plus haut, la suite des nombres naturels, puis on forme le tableau

4	3	2	1
0	0	3	1

en procédant comme il suit : sous l'unité on place l'unité; de l'unité prise 12 fois, c'est-à-dire de 10 (qui maintenant veut dire *douze*, et non plus *dix*) on retranche 9 et l'on écrit le reste 3 sous le nombre 2; du produit 30 (lisez *trente-six* ou *trois fois douze*) on retranche encore 9 autant de fois que possible, ce qui donne pour reste zéro, car trente-six contient quatre fois exactement le nombre 9. Les restes suivants seront nuls. Il viendra donc 0 sous tous les chiffres restants.

D'où l'on conclut que tous les nombres, écrits dans le système duodécimal, pour lesquels la somme du premier chiffre de droite et du triple du second (il n'est pas besoin de s'occuper des autres puisqu'ils donnent 0) sera divisible par 9, seront eux-mêmes des multiples de 9.

On reconnaîtra aussi que, dans le même système de numération, tous les nombres dont la somme des chiffres est divisible par 11, sont eux-mêmes des multiples de 11.

Dans notre système décimal au contraire, pour qu'un nombre fût divisible par 11, il faudrait que la somme formée par le dernier chiffre, puis le décuple de l'avant-dernier, puis le chiffre précédent, puis le décuple du précédent, etc., donnât un multiple de 11.

Il serait facile de justifier ces deux règles et d'en obtenir d'autres. Mais si j'ai touché ce sujet c'est parce que je cédais volontiers à l'attrait de la nouveauté; maintenant je m'arrête de peur de fatiguer le lecteur en entrant dans trop de détails.

Texte 10 : Liebniz : arithmétique binaire.

Tout en nous familiarisant avec le maniement de la base deux (écriture des nombres, pratique des opérations), Leibniz nous en montre les avantages ; et à partir du décryptage, à l'aide du système binaire des hexagrammes chinois, il évoque son projet de créer une langue logique universelle : la Caractéristique.

LEIBNIZ : Explication de l'arithmétique binaire ... Communication à l'Académie des sciences. 1703 Opera Omnia Genève 1768, p. 223-227.

XXI.

EXPLICATION DE L'ARITHMETIQUE BINAIRE, QUI SE SERT DES SEULS CARACTÈRES 0 ET 1, AVEC DES REMARQUES SUR SON UTILITÉ, ET SUR CE QU'ELLE DONNE LE SENS DES ANCIENNES FIGURES CHINOISES DE FOHY.

Le calcul ordinaire d'Arithmétique se fait suivant la progression de dix en dix. On se sert de dix caractères, qui sont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, qui signifient zero, un et les nombres suivans jusqu'à neuf inclusivement. Et puis allant à dix, on recommence, et on écrit dix par 10, et dix fois dix ou cent par 100, et dix fois cent ou mille par 1000, et dix fois mille par 10000, et ainsi de suite.

Mais au lieu de la progression de dix en dix, j'ai employé depuis plusieurs années la progression la plus simple de toutes, qui va de deux en deux, ayant trouvé qu'elle sert à la perfection de la science des Nombres. Ainsi je n'y employe point d'autres caractères que que 0 et 1, et puis allant à deux, je recommence. C'est pourquoi deux s'écrit ici par 10, et deux fois deux ou quatre par 100, et deux fois quatre ou huit par 1000, et deux fois huit ou seize par 10000, et ainsi de suite. Voici la Table des Nombres de cette façon, qu'on peut continuer tant que l'on voudra.

0	0
1	1
10	2
11	3
100	4
101	5
110	6
111	7
1000	8
1001	9
1010	10
1011	11
1100	12
1101	13
1110	14
1111	15
10000	16
10001	17
10010	18
10011	19
10100	20
10101	21
10110	22
10111	23
11000	24
11001	25
11010	26
11011	27
11100	28
11101	29
11110	30
11111	31
100000	32

etc.

On voit ici d'un coup d'oeil la raison d'une proprieté célébre de la progression Géométrique double en Nombres entiers, qui porte que si on n'a qu'un de ces nombres de chaque degré, on en peut composer tous les autres nombres entiers au dessous du double du plus haut degré. Car ici, c'est comme si on disait par exemple, que 111 ou 7 est la somme de quatre, de deux et un, et que 1101 ou 13 est la somme de huit, quatre et un. Cette proprieté sert aux Essayeurs pour peser toutes sortes de masses avec peu de poids et pourroit servir dans les monnoyes pour donner plusieurs valeurs avec peu de piéces.

100	4
10	2
1	1
111	7

1000	8
100	4
1	1
1101	13

Cette expressions des Nombres étant établie, sert à faire très facilement toutes sortes d'opérations.

Pour l'Addition par exemple. ☽

110	7	101	5	1110	14
111	6	1011	11	10001	17
..		....			
1101	13	10000	16	11111	31

Pour la Soustraction.

1101	13	10000	16	11111	31
111	7	1011	11	10001	17
110	6	101	5	1110	14

Pour la Multiplication. ⊙

11	3	101	5	101	5
11	3	11	3	101	5
11		101		101	
11		101		1010	
1001	9	1111	15	11001	25

Pour la Division.

15	1111	101	5
3	1111		
	11		

Et toutes ces opérations sont si aisées, qu'on n'a jamais besoin de rien essayer ni deviner, comme il faut faire dans la division ordinaire. On n'a point besoin non plus de rien apprendre par coeur ici, comme il faut faire dans le calcul ordinaire, où il faut savoir, par exemple, que 6 et 7 pris ensemble font 13. et que 5 multiplié par 3 donne 15, suivant la Table d'une fois un est un, qu'on appelle Pythagorique. Mais ici tout cela se trouve et se prouve de source, comme l'on voit dans les exemples précédens sous les signes ☽ et ⊙.

Cependant je ne recommande point cette manière de compter, pour la faire introduire à la place de la pratique ordinaire par dix. Car outre qu'on est accoutumé à celle-ci, on n'y a point besoin d'y apprendre ce qu'on a déjà appris par cœur: ainsi la pratique par dix est plus abregée, et les nombres y sont moins longs. Et si on étoit accoutumé à aller par douze ou par seize, il y auroit encore plus d'avantage. Mais le calcul par deux, c'est-à-dire par 0 et par 1, en récompense de sa longueur, est le plus fondamental pour la science, et donne de nouvelles découvertes, qui se trouvent utiles ensuite, même pour la pratique des nombres, et surtout pour la Géométrie, dont la raison est que les nombres étant reduits aux plus simples principes, comme 0 et 1, il paroit partout un ordre merveilleux. Pour exemple, dans la Table même des Nombres, on voit en chaque colonne régner des périodes qui recommencent toujours. Dans la première colonne c'est 01, dans la seconde 0011, dans la troisième 00001111, dans la quatrième 0000000011111111, et ainsi de suite. Et on a mis de petits zéros dans la Table pour remplir le vuide au commencement de la colonne, et pour mieux marquer ces périodes. On a mené aussi des lignes dans la Table, qui marquent que ce que ces lignes renferment revient toujours sous elles. Et il se trouve encore que les Nombres Quarrés, Cubiques et d'autres puissances, item les Nombres Triangulaires, Pyramidaux et d'autres nombres figurés, ont aussi de semblables périodes, de sorte qu'on en peut écrire les Tables tout de suite, sans calculer. Et une prolixtié dans le commencement, qui donne ensuite le moyen d'epargner le calcul et d'aller à l'infini par règle, est infiniment avantageuse.

Ce qu'il y a de surprenant dans ce calcul, c'est que cette Arithmétique par 0 et 1 se trouve contenir le mystère des lignes d'un ancien Roi et Philosophe nommé Fohy, qu'on croit avoir vécu il y a plus de quatre mille ans et que les Chinois regardent comme le Fondateur de leur Empire et de leurs sciences. Il y a plusieurs figures linéaires qu'on lui attribue, elles reviennent toutes à cette Arithmétique; mais il suffit de mettre ici la Figure de huit Cova comme on l'appelle, qui passe pour fondamentale, et d'y joindre l'explication qui est manifeste, pourvû qu'on remarque premièrement qu'une ligne entière — signifie l'unité ou 1, et secondement qu'une ligne brisée -- signifie le zéro ou 0.

☷	000	0	0
☶	001	1	1
☵	010	10	2
☴	011	11	3
☳	100	100	4
☲	101	101	5
☱	110	110	6
☰	111	111	7

Les Chinois ont perdu la signification des Cova ou Linéations de Fohy, peut-être depuis plus d'un millenaire d'années, et ils ont fait des Commentaires la-dessus, où ils ont cherché je ne scai quels sens éloignés, de sorte qu'il a fallu que la vraie explication leur vint maintenant des Européens. Voici comment: Il n'y a guères plus de deux ans que j'envoyai au R. P. Bouvet, Jésuite Français célèbre, qui demeure à Pekin, ma manière de compter par 0 et 1, et il n'en fallut pas davantage pour lui faire reconnaitre que c'est la clef des figures de Fohy. Ainsi m'écrivant le 14 Novembre 1701, il m'a envoyé la grande figure de ce Prince Philosophe qui va à 64, et ne laisse plus lieu de douter de la vérité de notre interprétation, de sorte qu'on peut dire que ce Père a déchiffré l'enigme de Fohy, à l'aide de ce que je lui avois communiqué. Et comme ces figures sont peut-être le plus ancien monument de

science qui soit au monde, cette restitution de leur sens, après un si grand intervalle de tems, paroitra d'autant plus curieuse.

Le consentement des figures de Fohy et ma Table des Nombres se fait mieux voir, lorsque dans la Table on supplée les zéros initiaux, qui paroissent superflus, mais qui servent à mieux marquer la période de la colonne, comme je les y ai supplées en effet avec des petits ronds pour les distinguer des zéros nécessaires, et cet accord me donne un grande opinion de la profondeur des méditations de Fohy. Car ce qui nous paroit aisé maintenant, ne l'étoit pas tout dans ces tems éloignés. L'Arithmétique Binaire ou Dyadique est en effet fort aisée aujourd'hui, pour peu qu'on y pense, parce que notre manière de compter y aide beaucoup, dont il semble qu'on retranche seulement le trop. Mais cette Arithmétique ordinaire pour dix ne paroit pas fort ancienne, au moins les Grecs et les Romains l'ont ignorée et ont été privés de ses avantages. Il semble que l'Europe en doit l'introduction à Gerbert, depuis Pape sous le nom de Sylvestre II, qui l'a eue des Maures d'Espagne.

Or comme l'on croit à la Chine que Fohy est encore auteur des caractères Chinois, quoique fort altérés par la suite des tems; son essai d'Arithmétique fait juger qu'il pourroit bien s'y trouver encore quelque chose de considerable par rapport aux nombres et aux idées, si l'on pouvoit déterrer le fondement de l'écriture Chinoise, d'autant plus qu'on croit à la Chine, qu'il a eu égard aux nombres en l'établissant. Le R. P. Bouvet est fort porté à pousser cette pointe, et très capable d'y réussir en bien des manières. Cependant je ne sçai s'il y a jamais eu dans l'écriture Chinoise un avantage approchant de celui qui doit être necessairement dans une Caractéristique que je projette. C'est que tout raisonnement qu'on peut tirer des notions, pourroit être tiré de leurs Caractères par une manière de calcul, qui seroit un des plus importans moyens d'aider l'esprit humain.

Note : Pour les nombres figurés (carré, triangulaire) voir Nicomaque de Gérase § 3, texte 3.

Les cubes sont évidemment : 1, 8, 27, 64 ...

Pour les pyramidaux voici la définition de Nicomaque de Gérase (livre II, chapitre XIII) : " Les pyramides partant d'une base triangle sont donc, en bon ordre, les suivantes :

1, 4, 10, 20, 35, 56, 84

et la suite, dont la génése est l'entassement, les uns sur les autres, des nombres triangles eux-mêmes, d'abord 1, puis 1 et 3, puis 1, 3, 6, puis, en plus de ceux-ci, 10, et dans la suite, avec les précédents, 15 et en outre 21 et à la suite 28, et à l'infini. "

- LE RENOUVEAU DE LA THEORIE DES NOMBRES.

Texte 11 : FERMAT : la descente infinie.

Au 17^{e} siècle, l'arithmétique spéculative retrouve une nouvelle vigueur, en renouant naturellement avec les méthodes et les problèmes légués par l'Antiquité grecque, en premier lieu Diophante. Pierre FERMAT est l'un des acteurs de ce renouveau. Conseiller au Parlement de Toulouse, il n'a pas laissé d'ouvrage complétement rédigé. Son oeuvre mathématique est composée de lettres et de notes fort peu détaillées.

Le texte suivant est peut-être celui qui fournit le plus d'indications sur les méthodes mises en oeuvre par FERMAT. Le problème posé consiste à prouver que l'aire d'un triangle rectangle dont les côtés sont mesurés par des nombres entiers ne peut être le carré d'un nombre entier : par exemple, le célèbre triangle 3-4-5 a une aire égale à 30.

Depuis Euclide, les côtés d'un tel triangle sont connus. En langage actuel, nous dirons que les solutions de l'équation diophantienne $x^2 + y^2 = z^2$ sont de la forme $x = 2\lambda mn$, $y = \lambda(m^2 - n^2)$, $z = \lambda(m^2 + n^2)$ où m et n sont des entiers premiers entre eux, l'un pair et l'autre impair. Si $\lambda = 1$, le triangle est dit primitif, il a ses côtés premiers entre eux : c'est ce cas qu'envisage FERMAT.

L'aire de ce triangle est $mn(m^2 - n^2)$, produit de trois facteurs deux à deux premiers entre eux. Si cette aire était un carré, on aurait : $m = a^2$, $n = b^2$, $m^2 - n^2 = c^2$, d'où $a^4 - b^4 = c^2$: " il y aurait deux bicarrés dont la différence serait un carré ". La suite d'entend de même : l'égalité $a^4 - b^4 = c^2$ s'écrit $(a^2 - b^2)(a^2 + b^2) = c^2$ et donc $a^2 - b^2 = \alpha^2$, $a^2 + b^2 = \beta^2$, ce qui équivaut à : $\alpha^2 + 2b^2 = \beta^2$, $\alpha^2 + b^2 = a^2$.

FERMAT sait résoudre l'équation diophantienne $\alpha^2 + 2b^2 = \beta^2$; il dit que l'on a alors $\beta = k^2 + 2h^2$, et devrait ajouter : $\alpha = k^2 - 2h^2$, $b = 2kh$. Si l'on pose $u = k^2$ et $v = 2h^2$, on voit bien alors que u et v sont les côtés de l'angle droit d'un nouveau triangle rectangle, car on a :

$$u^2 + v^2 = k^4 + 4h^4 = \alpha^2 + b^2 = a^2$$

L'aire de ce nouveau triangle est $\frac{1}{2}uv = (kh)^2$: c'est un carré ! FERMAT lui applique le même raisonnement qu'au triangle initial, et observe que l'on doit avoir $u = m_1^2 - n_1^2$, $v = 2m_1n_1$, $a = m_1^2 + n_1^2$. Mais si l'on se souvient que $v = 2h^2$, on voit que $m_1n_1 = h^2$ et donc m_1 et n_1 sont encore des carrés : $m_1 = a_1^2$, $n_1 = b_1^2$. Reportant ceci dans l'égalité $u = m_1^2 - n_1^2$, il

vient : $a_1^4 - b_1^4 = u = k^2$, d'où deux nouveaux carrés, a_1^2 et b_1^2 , dont la somme et la différence sont des carrés : même situation que précédemment, avec des nombres strictement plus petits. Ceci conduit à une impossibilité. C'est la méthode de descente infinie dont nous avons vu un exemple précédemment (texte n°6 § 3).

FERMAT : Oeuvres tome III p. 271-272.
Traduction P. Tannery. Paris 1896.

45. — Problème 20 de Bachet sur Diophante, VI, 26.

« Bachet. — Trouver un triangle rectangle dont l'aire soit un nombre donné. »

L'aire d'un triangle rectangle en nombres ne peut être un carré.

Je vais donner la démonstration de ce théorème que j'ai découvert; je ne l'ai pas trouvée au reste sans une pénible et laborieuse méditation; mais ce genre de démonstration conduira à des progrès merveilleux dans la science des nombres.

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

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

Par le même raisonnement, on aura ensuite une autre somme plus petite que celle déduite de la première, et en continuant indéfiniment on trouvera toujours des nombres entiers de plus en plus petits satisfaisant aux mêmes conditions. Mais cela est impossible, puisqu'un nombre entier étant donné, il ne peut y avoir une infinité de nombres entiers qui soient plus petits.

La marge est trop étroite pour recevoir la démonstration complète et avec tous ses développements.

Par le même procédé, j'ai découvert et démontré qu'il n'y a aucun nombre triangulaire, sauf l'unité, qui soit un bicarré.

Texte 12 : LEGENDRE : la réciprocité quadratique.

Nous venons de voir que Fermat a repris le flambeau de la théorie des nombres en s'attaquant aux problèmes légués par Diophante. De même, à sa suite, Euler et Lagrange ont réexaminé des problèmes posés par Fermat, en ont donné des solutions et des généralisations, et ont restitué des démonstrations absentes des écrits du mathématicien occitan. Citons par exemple le " petit théorème de Fermat ", démontré et généralisé par Euler, qui affirme que si le nombre naturel premier p ne divise pas l'entier a, alors il divise $a^{p-1} - 1$.

Le texte qui suit est le début de l'article IV d'un mémoire présenté par Legendre à l'Académie des Sciences en 1785. Il montre que les recherches étaient encore très actives autour de la question de la représentation des entiers sous certaines " formes quadratiques ", ou des diviseurs de telles formes. Si a désigne un entier quelconque et p un nombre premier impair, Legendre observe que p divise $t^2 - au^2$, avec t et u premiers entre eux, si et seulement si le nombre $a^{\frac{p-1}{2}}$ donne comme reste 1 lorsqu'on le divise par p. Dans le cas contraire, ce reste est égal à p-1, d'après le petit thérorème de Fermat. Legendre note respectivement ces deux cas : $a^{\frac{p-1}{2}} = 1$ et $a^{\frac{p-1}{2}} = -1$, ce qui, dit-il, " suppose qu'on a rejeté les multiples de p dans le premier membre " (notons ici l'anticipation sur les congruences de Gauss).

Cela dit, si c et d sont deux nombres premiers impairs, il existe une relation entre les valeurs de $c^{\frac{d-1}{2}}$ et $d^{\frac{c-1}{2}}$, relation que Legendre consigne dans les théorèmes qui terminent le présent extrait. Cette relation a été nommée plus tard loi de réciprocité quadratique et elle a eu une grande importance dans la Théorie des Nombres au 19e siècle. Par la suite, Legendre perfectionnera son exposé : il notera $(\frac{a}{p})$ la valeur + 1 ou - 1 de $a^{\frac{p-1}{2}}$ " modulo p ", et sa loi s'écrira :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} ,$$

où p et q sont les nombres premiers impairs notés ici c et d ou bien a, A, b, B, selon les cas. Les huits théorèmes du présent texte s'exprimeront dans cette unique formule, mais Legendre n'en trouvera jamais une véritable et complète démonstration : c'est Gauss qui le fera.

LEGENDRE : Mémoires de l'Académie Royale des Sciences. 1785.

ARTICLE IV.

Contenant divers Théorèmes ſur les Nombres premiers.

ON doit regretter beaucoup que Fermat, qui avoit cultivé avec un grand ſuccès la théorie des nombres, ne nous ait pas laiſſé la démonſtration des théorèmes auxquels il étoit parvenu. À la vérité, M.rs Euler & de la Grange, qui n'ont pas dédaigné ce genre de recherches, ont démontré la plupart de ces théorèmes, & ont même ſubſtitué des théories très-étendues aux propoſitions iſolées de Fermat; mais il en eſt pluſieurs qui ont réſiſté à leurs efforts, ſoit que Fermat n'en eût pas réellement une démonſtration ſolide, ce qui eſt difficile à croire, ſoit que l'inſtrument pour y parvenir nous ſoit encore tout-à-fait inconnu. Parmi ces propoſitions non démontrées, on doit remarquer ſur-tout les deux ſuivantes: *tout nombre eſt compoſé de trois triangulaires au plus: tout nombre premier de la forme* $8n - 1$, *eſt de la forme* $p^2 + q^2 + 2r^2$, *ou, ce qui revient au même, ſon double eſt la ſomme de trois carrés.* Mais j'obſerve à l'égard de celle-ci, qu'elle ne caractériſe nullement les nombres premiers de la forme $8n - 1$, car il n'eſt aucun nombre impair, ſimple ou compoſé, qui ne ſoit de la forme mentionnée, & même qui ne ſoit à la fois des deux formes $p^2 + q^2 + r^2$, $p^2 + q^2 + 2r^2$, excepté ſeulement les nombres (premiers ou non) de la forme $8n - 1$, qui ne peuvent être de la première forme $p^2 + q^2 + r^2$, mais qui ſont toujours de la ſeconde $p^2 + q^2 + 2r^2$. Néanmoins la propoſition de Fermat ſeroit d'autant plus intéreſſante à démontrer, qu'il en réſulteroit, d'une manière fort directe, que tout nombre eſt la ſomme de quatre carrés: en effet, les nombres premiers $8n - 3$ ſont de la forme $p^2 + q^2$, les nombres premiers $8n + 3$ ſont de la forme $p^2 + 2q^2$, les nombres premiers $8n + 1$. ſont à la fois des deux formes $p^2 + q^2$, $p^2 + 2q^2$. Ces propoſitions ſont connues & démontrées: ſi donc les nombres premiers $8n - 1$ ſont de la forme $p^2 + q^2 + 2r^2$, il s'enſuivra qu'un nombre quelconque eſt la ſomme de quatre carrés au plus; car on ſait d'ailleurs que le produit des deux formules $a^2 + b^2 + c^2 + d^2$, & $p^2 + q^2 + r^2 + s^2$, eſt également la ſomme de quatre carrés.

Au reſte, il n'y a pas de doute que tout nombre ne

ſoit compoſé de quatre carrés, puiſque cette propoſition a été démontrée par M. de la Grange, dans les Mémoires de Berlin, *année 1772 ;* & enſuite un peu plus ſimplement par M. Euler, dans les actes de Léipſick, *année 1773*. Mais il eſt remarquable que cette propoſition ſuive également de l'une ou de l'autre des deux déjà citées ; car ſi l'on ſuppoſe que tout nombre eſt la ſomme de trois triangulaires, il s'enſuivra que tout nombre de la forme $8n + 3$ eſt la ſomme de trois carrés $p^2 + q^2 + r^2$; donc on peut toujours ſuppoſer $8n + 4 = p^2 + q^2 + r^2 + 1$; d'où il ſuit que $2n + 1$, c'eſt-à-dire, tout nombre impair ſera la ſomme de quatre carrés, & conſéquemment auſſi tout nombre pair.

Mais je dis plus, les quatre carrés peuvent ſe réduire à trois, ou au moins deux des quatre peuvent être ſuppoſés égaux. De ſorte que *tout nombre, ou au moins ſon double, eſt la ſomme de trois carrés ;* ſouvent même le nombre & ſon double ſeront à la fois la ſomme de trois carrés ; c'eſt ce qui arrive généralement aux nombres impairs, comme nous l'avons déjà dit, excepté ceux de la forme $8n - 1$, dont le double ſeulement eſt la ſomme de trois carrés. Ces propoſitions que j'indique en paſſant, acquerront par la ſuite un plus grand degré de probabilité ; mais ce n'eſt pas l'objet principal que j'ai en vue.

M. de la Grange a conſidéré d'une manière générale (*Mém. de Berlin 1773 & 1775*), les diviſeurs de la formule $t^2 \pm au^2$, & il en a déduit par rapport aux nombres premiers une multitude de théorèmes intéreſſans. Les recherches de ce grand géomètre, m'ont engagé à conſidérer plus particulièrement le cas où a eſt un nombre premier dans la formule $t^2 + au^2$, & à l'aide du théorème de l'*article III*, je ſuis parvenu à démontrer des propoſitions très-générales ſur les nombres premiers, propoſitions qui paroiſſent avancer cette partie de l'analyſe & mériter l'attention des géomètres.

1. Comme il ſera principalement queſtion des nombres premiers dans ce qui ſuit, & que leurs différentes formes donnent lieu à différentes propriétés, nous déſignerons par A, a, α, A' &c. ceux de la forme $4n + 1$, par B, b, β, C, B', &c. ceux de la forme $4n - 1$, & par les autres lettres, ceux dont la forme n'eſt pas déterminée. Nous avertiſſons auſſi que cette expreſſion $\partial^{\frac{\epsilon-1}{2}} = 1$ ou -1, ſuppoſe qu'on a rejeté les multiples de ϵ dans le premier membre. Or, quel que ſoit ∂, premier ou non, pourvu qu'il ne ſoit pas multiple du nombre premier ϵ, on doit avoir ou $\partial^{\frac{\epsilon-1}{2}} = 1$, ou $\partial^{\frac{\epsilon-1}{2}} = -1$. De ſorte que, par rapport au nombre premier ϵ, tous les nombres non diviſibles par ϵ, ſe partagent en deux claſſes également nombreuſes, l'une qui ſatisfait à l'é-

quation $\partial^{\frac{c-1}{2}} = 1$, l'autre qui satisfait à l'équation $\partial^{\frac{c-1}{2}} = -1$. Enfin, nous rappellerons ce qui est démontré fort au long dans l'*article I*, que si la formule $t^2 + \partial u^2$ est divisible par le nombre premier c, il faut qu'on ait $(-\partial)^{\frac{c-1}{2}} = +1$. Donc, si on avoit $(-\partial)^{\frac{c-1}{2}} = -1$, on seroit sûr que c ne peut pas diviser la formule $t^2 + \partial u^2$, formule où l'on suppose toujours t & u des indéterminées, telles cependant que t & ∂u n'ont point de commun diviseur.

THÉORÈME I.

Si $b^{\frac{a-1}{2}} = 1$, il s'ensuit $a^{\frac{b-1}{2}} = 1$.

THÉORÈME II.

Si $a^{\frac{b-1}{2}} = -1$, il s'ensuit $b^{\frac{a-1}{2}} = -1$.

THÉORÈME III.

Si $a^{\frac{A-1}{2}} = 1$, il s'ensuit $A^{\frac{a-1}{2}} = 1$.

THÉORÈME IV.

Si $a^{\frac{A-1}{2}} = -1$, il s'ensuit $A^{\frac{a-1}{2}} = -1$.

THÉORÈME V.

Si $a^{\frac{b-1}{2}} = 1$, il s'ensuit $b^{\frac{a-1}{2}} = 1$.

THÉORÈME VI.

Si $b^{\frac{a-1}{2}} = -1$, il s'ensuit $a^{\frac{b-1}{2}} = -1$.

THÉORÈME VII.

Si $b^{\frac{B-1}{2}} = 1$, il s'ensuit $B^{\frac{b-1}{2}} = -1$.

THÉORÈME VIII.

Si $b^{\frac{B-1}{2}} = -1$, il s'ensuit $B^{\frac{b-1}{2}} = 1$.

Ces Théoremes ainsi détaillés, sont encore d'une grande généralité, mais on auroit pu les comprendre tous dans l'énoncé suivant.

c & ∂ étant deux nombres premiers, les expressions $c^{\frac{\partial-1}{2}}$, $\partial^{\frac{c-1}{2}}$ ne seront de différens signes que lorsque c & ∂ seront tous deux de la forme $4n - 1$; dans tous les autres cas, ces expressions auront toujours le même signe.

On sait d'ailleurs que chacune en particulier, ne peut être que $+1$ ou -1, ainsi il n'y a pas d'embarras sur le sens de ce théorème.

Texte 13 : GAUSS : les congruences.

En 1801, GAUSS, âgé de 24 ans, fait paraître ses " Recherches Arithmétiques ", dont voici le tout début. Il s'agit d'un ouvrage fondamental, qui a dominé tout le 19e siècle. Gauss reprend les résultats connus de la Théorie des Nombres, mais il les expose d'une manière ordonnée et rigoureuse, en présentant des méthodes, des notations et des concepts nouveaux qui lui servent à démontrer plus efficacement les résultats de Fermat, Euler, Lagrange, Legendre, et surtout à étendre plus loin le champ de ses investigations. Comme nous le voyons ici, il commence par définir la notion de congruence, devenue depuis indispensable. Dans une note, il observe que Legendre avait bien perçu la nécessité d'une telle notion, mais qu'il avait utilisé le signe = pour la représenter : c'est ce que nous avions vu dans le texte précédent.

On notera le caractère très " moderne " de ce texte, qui le rend immédiatement accessible à un lecteur d'aujourd'hui.

GAUSS : Recherches Arithmétiques. 1801. Pages 1 à 5.
Traduction Poullet-Delisle. Blanchard 1963.

SECTION PREMIÈRE.

Des Nombres congrus en général.

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire, sans aucun signe.

Ainsi -9 et $+16$ sont *congrus* par rapport au module 5; -7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné a suivant le module m, sont compris dans la formule $a + km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer

peuvent sans peine se démontrer par-là; mais chacun en sentira la vérité au premier aspect.

Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses; ainsi $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$ (*).

3. THÉORÈME. *Soient* m *nombres entiers successifs* a, $a+1$, $a+2$, ... $a+m-1$ *et un autre* A, *un des premiers sera congru avec* A, *suivant le module* m, *et il n'y en aura qu'un.*

En effet, si $\frac{a-A}{m}$ est entier, on aura $a \equiv A$; s'il est fractionnaire, soit k le nombre entier immédiatement plus grand ou plus petit, suivant que $\frac{a-A}{m}$ sera positif ou négatif, en ne faisant point d'attention au signe, $A+km$ tombera nécessairement entre a et $a+m$; ce sera donc le nombre cherché. Or il est évident que les quotiens $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, etc., sont compris entre $k-1$ et $k+1$, donc un seul d'entr'eux peut être entier.

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, \ldots (m-1)$, que dans celle-ci $0, -1, -2, \ldots -(m-1)$; nous les appellerons résidus *minima*; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu *minimum absolu*.

Par exemple -13 suivant le module 5, a pour résidu *minimum* positif 2, qui est en même temps *minimum absolu*, et -3 pour résidu *minimum* négatif; $+5$, suivant le module 7, est lui-même son résidu *minimum* positif; -2 est le résidu *minimum* négatif et en même temps le *minimum absolu*.

5. Des notions que nous venons d'établir, nous tirerons d'abord les conséquences suivantes :

Les nombres qui sont congrus suivant un module composé, le sont également suivant un quelconque de ses diviseurs.

Si plusieurs nombres sont congrus à un même suivant le même module, ils seront congrus entre eux (toujours suivant le même module).

On doit supposer la même identité de module dans ce qui suit.

Les nombres congrus ont les mêmes résidus minima; *les nombres incongrus les ont différens.*

(*) Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence; nous en avons préféré un autre, pour prévenir toute ambiguité.

6. *Si les nombres* A, B, C, *etc.*; a, b, c, *etc. sont congrus chacun à chacun, c'est-à-dire, si* $A \equiv a$, $B \equiv b$, *etc. on aura...*

$$A + B + C + \text{etc.} \equiv a + b + c + \text{etc.}$$

Si $A \equiv a$, $B \equiv b$, on a aussi $A - B \equiv a - b$.

7. *Si* $A \equiv a$, *on a aussi* $kA \equiv ka$.

Si k est positif, ce n'est qu'un cas particulier de l'article précédent, en posant $A = B = C$, etc., $a = b = c$, etc.

Si k est négatif, $-k$ sera positif; donc $-kA \equiv -ka$, et partant $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, $AB \equiv ab$; car $AB \equiv Ab \equiv ba$.

8. Si les nombres A, B, C, etc., a, b, c, etc. sont congrus chacun à chacun, les produits ABC, etc., et abc, etc. seront congrus.

Par l'article précédent, $AB \equiv ab$; par la même raison $ABC \equiv abc$, et ainsi de suite.

En prenant tous les nombres A, B, C, etc., égaux entr'eux, ainsi que les correspondans a, b, c, etc., on déduit ce théorème:

Si $A \equiv a$ *et que* k *soit entier positif, on aura* $A^k \equiv a^k$.

9. *Soit* X *une fonction de l'indéterminée* x, *de cette forme....* $Ax^c + Bx^b + Cx^c$, *etc.*, A, B, C, *etc, étant des nombres entiers quelconques*, a, b, c, *etc. des nombres entiers positifs. Si l'on donne à* x *des valeurs congrues, suivant un certain module, les valeurs résultantes pour* X, *le seront aussi.*

Soient f et g les valeurs congrues de x; par les articles précédens $f^c \equiv g^c$ et $Af^c \equiv Ag^c$; de même $Bf^b \equiv Bg^b$, etc. : donc

$$Af^c + Bf^b + Cf^c + \text{etc.} \equiv Ag^c + Bg^b + Cg^c + \text{etc.}$$

Au reste on conçoit aisément que ce théorème peut s'étendre à des fonctions de plusieurs indéterminées.

10. Si donc on substitue à la place de x tous les nombres entiers consécutifs, et que l'on cherche les résidus *minima* des valeurs de X, ils formeront une suite dans laquelle, après un intervalle de m termes (m étant le module), les mêmes termes se représenteront; c'est-à-dire que cette suite sera formée d'une période de m termes répétée indéfiniment.

Soit par exemple: $X = x^3 - 8x + 6$ et $m = 5$, pour $x = 0, 1, 2, 3$, etc. les valeurs de X donnent pour résidus *minima* positifs : 1, 4, 3, 4, 3, 1, 4, etc., où les cinq premiers 1, 4, 3, 4, 3 se répètent indéfiniment; et si l'on continue la série en sens contraire, c'est-à-dire, si l'on donne à x des valeurs négatives, la même période reparaît en sens inverse; d'où il suit que la série ne renferme pas d'autres termes que ceux qui composent la période.

11, Donc dans cet exemple, X ne peut devenir $\equiv 0$, ni $\equiv 2$, (mod. 5), et encore moins $= 0$ ou $= 2$, d'où il suit que les équations $x^3 - 8x + 6 = 0$ et $x^3 - 8x + 4 = 0$ n'ont point de racines entières, et parconséquent point de racines rationnelles. On voit en général que lorsque X est de la forme $x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$; A, B, C, etc. étant entiers, et n entier positif, l'équation $X = 0$,

(forme à laquelle toute équation algébrique peut se ramener) n'aura aucune racine rationnelle, s'il arrive que pour un certain module la congruence $X \equiv 0$ ne soit pas satisfaite ; mais ce caractère qui se présente ici de lui-même, sera développé davantage dans la section VIII. On peut au moins se former par cette esquisse une idée de l'utilité de nos recherches.

12. Plusieurs des théorèmes que l'on a coutume d'exposer dans les traités d'arithmétique, s'appuient sur ceux que nous avons présentés ; par exemple, la règle pour reconnaître si un nombre est divisible par 9, 11, ou tout autre nombre. Suivant le module 9 toutes les puissances de 10 sont congrues à l'unité ; donc si le nombre est de la forme $a + 10b + 100c + 1000d + \text{etc.}$, il aura, suivant le module 9, le même résidu *minimum* que $a + b + c + \text{etc.}$ Il est clair d'après cela, que si l'on ajoute les figures du nombre, sans avoir égard au rang qu'elles occupent, la somme que l'on obtiendra, et le nombre proposé auront les mêmes résidus *minima* ; si donc ce dernier est divisible par 9, la somme des chiffres le sera aussi, et seulement dans ce cas. Il en est de même du diviseur 3. Comme suivant le module 11, $100 \equiv +1$, on aura généralement $10^{2\mu} \equiv 1$, $10^{2\mu+1} \equiv 10 \equiv -1$, et le nombre de la forme $a + 10b + 100c + \text{etc.}$, aura le même résidu *minimum* que $a - b + c - \text{etc.}$; d'où dérive sur-le-champ la règle connue. On déduira facilement du même principe toutes les règles semblables.

Ce qui précède donne encore la raison des règles que l'on prescrit ordinairement pour la vérification des opérations arithmétiques ; savoir, lorsque de nombres donnés on doit en déduire d'autres par addition, soustraction, multiplication ou élévation aux puissances. On n'a qu'à substituer dans les opérations, à la place des nombres donnés, leurs résidus *minima*, suivant un module quelconque (ordinairement 9 ou 11, parceque dans le système décimal, comme nous venons de le voir, on trouve facilement les résidus relatifs à ces modules) ; les nombres résultans devront être congrus à ceux qu'on déduirait des nombres donnés, sinon il y aurait un vice dans le calcul.

Mais il serait superflu de nous arrêter plus long-temps sur ces résultats très-connus, ainsi que sur ceux du même genre.

5 - VERS LES FONDEMENTS.

Ce n'est qu'au XIXe siècle que les mathématiciens ébranlés par l'apparition des géométries non euclidiennes (voir Géométrie), se défiant de l'intuition, cherchèrent pour leurs théories des modèles fondés sur l'arithmétique. Mais la réflexion entamée sur les fondements des mathématiques les amenèrent à se pencher sur les fondements de l'arithmétique elle-même. Dans le premier texte qui suit, Leibniz fait figure de précurseur. Dans le texte suivant Frege, qui reprend l'exemple de Leibniz, met en évidence des propriétés de d'addition dans l'ensemble des entiers et la possibilité d'une axiomatisation de N. Celle-ci sera réalisée quelques années plus tard : la plus connue est celle de Peano (voir sa première version en illustration). Un des axiomes, et qui joue un rôle essentiel, est le principe de récurrence. Ce dernier utilisé pour la première fois par Pascal de façon explicite (voir encadré) est devenu d'un usage courant en arithmétique, comme en combinatoire ou en analyse (suites et séries). Dans le dernier texte Poincaré en fait saisir le mécanisme et l'intérêt.

Texte 14 : Leibniz : deux plus deux égale quatre.

LEIBNIZ : Nouveaux Essais dur l'Entendement Humain.
Ecrits en 1703, publiés en 1765. Livre IV, chapitre VII, § 10.

PHILALÈTHE. Notre habile auteur dit ici : Je voudrais bien demander à ces Messieurs, qui prétendent que toute autre connaissance (qui n'est pas de fait) dépend des principes généraux innés et évidents par eux-mêmes, de quel principe ils ont besoin pour prouver que *deux et deux est quatre ?* car on connaît (selon lui) la vérité de ces sortes de propositions sans le secours d'aucune preuve. Qu'en dites-vous, Monsieur ?

THÉOPHILE. Je dis que je vous attendais là bien préparé. Ce n'est pas une vérité tout à fait immédiate que deux et deux sont quatre, supposé que *quatre* signifie trois et un. On peut donc la démontrer, et voici comment :

Définitions :

1) *Deux* est un et un.
2) *Trois* est deux et un.
3) *Quatre* est trois et un.

Axiome. Mettant des choses égales à la place, l'égalité demeure.

Démonstration :

2 et 2 est 2 et 1 et 1 (par la déf. 1) ..... 2 + 2
2 et 1 et 1 est 3 et 1 (par la déf. 2)..... 2 + 1 + 1
3 et 1 est 4 (par la déf. 3) ..... 3 + 1
4

Donc (par l'axiome)
2 et 2 est 4. Ce qu'il fallait démontrer.

Je pouvais, au lieu de dire que 2 et 2 est 2 et 1 et 1, mettre que 2 et 2 est égal à 2 et 1 et 1, et ainsi des autres. Mais on le peut sous-entendre partout, pour avoir plus tôt fait; et cela en vertu d'un autre axiome qui porte qu'une

chose est égale à elle-même, ou que ce qui est le même est égal.

PHILALÈTHE. [Cette démonstration, quelque peu nécessaire qu'elle soit par rapport à sa conclusion trop connue, sert à montrer comment les vérités ont de la dépendance des définitions et des axiomes. Ainsi je prévois ce que vous répondrez à plusieurs objections qu'on fait contre l'usage des axiomes. On objecte qu'il y aura une multitude innombrable de principes; mais c'est quand on compte entre les principes les corollaires qui suivent des définitions avec l'aide de quelque axiome. Et puisque les définitions ou idées sont innombrables, les principes le seront aussi dans ce sens, et supposant même avec vous que les principes indémontrables sont les axiomes identiques. Ils deviennent innombrables aussi par l'exemplification, mais dans le fond on peut compter A est A, et B est B pour un même principe revêtu diversement.

THÉOPHILE. De plus cette différence des degrés qu'il y a dans l'évidence fait que je n'accorde point à votre célèbre auteur que toutes ces vérités, qu'on appelle *principes*, et qui passent pour évidentes par elles-mêmes, parce qu'elles sont si voisines des premiers axiomes indémontrables, sont entièrement indépendantes et incapables de recevoir les unes des autres aucune lumière ni preuve. Car on les peut toujours réduire ou aux axiomes mêmes, ou à d'autres vérités plus voisines des axiomes, comme cette vérité que deux et deux font quatre vous l'a fait voir

Texte 15 : Frege : peut-on démontrer les formules numériques ?

FREGE : Les fondements de l'arithmétique. 1884, chapitre 1, § 1.

Traduction : C. Imbert, Seuil 1969.

LES FONDEMENTS DE L'ARITHMÉTIQUE

5. Il faut distinguer entre les formules numériques telles que $2 + 3 = 5$, qui portent sur des nombres déterminés, et les lois générales qui valent pour tous les nombres entiers.

Quelques philosophes ont tenu les premières pour indémontrables et immédiatement claires comme des axiomes. Kant les déclare indémontrables et synthétiques, mais il a scrupule à les nommer axiomes parce qu'elles ne sont pas générales et que leur nombre est infini. Hankel , à juste titre, refuse d'admettre un nombre infini de vérités premières indémontrables et voit là un paradoxe : il contredirait en effet au besoin qu'éprouve la raison de dominer les premiers fondements. Voit-on immédiatement que :

$$135\,664 + 37\,863 = 173\,527?$$

Non. Et c'est bien la raison que donne Kant en faveur de la nature synthétique de ces propositions. Mais elle parle plus encore contre leur indémontrabilité. Comment seraient-elles comprises autrement que par une preuve, si leur vérité n'éclate pas immédiatement? Kant veut s'aider de l'intuition de doigts ou de points, en quoi il court le risque de donner un aspect empirique à ces propositions, à l'encontre de ce qu'il pense. Car l'intuition de 37 863 doigts n'est certainement pas une intuition pure. Il semble même que le terme d' « intuition » ne convienne pas, car si l'on tient compte de la manière de les grouper, 10 doigts peuvent déjà donner lieu aux intuitions les plus variées. Avons-nous vraiment une intuition de 135 664 doigts ou points? Alors et si nous avions aussi une intuition de 37 863 doigts, puis une encore de 173 527, la justesse de notre équation, à la supposer non démontrable, devrait apparaître d'emblée, au moins pour les doigts; mais tel n'est pas le cas.

Visiblement, Kant ne pensait qu'aux petits nombres. Les formules qui portent sur les grands nombres pourraient faire l'objet d'une démonstration tandis qu'elles seraient immédiatement comprises par l'intuition quand elles portent sur de petits nombres. Mais il est bien périlleux de faire une différence fondamentale entre petits et grands nombres, pour cette raison surtout qu'on ne saurait marquer la frontière, sinon grossièrement. Si les formules numériques étaient démontrables à partir de 10 par exemple, il serait juste de demander : pourquoi pas à partir de 5, de 2 ou de 1?

6. D'autres philosophes et mathématiciens n'ont pas hésité à affirmer qu'on pouvait démontrer les formules numériques. Leibniz dit :

« Ce n'est pas une vérité immédiate que 2 et 2 font 4. Supposé que 4 désigne 3 et 1, on peut le démontrer ainsi.

Définitions : 1) 2 est 1 et 1
2) 3 est 2 et 1
3) 4 est 3 et 1

Axiome : Quand on substitue des égaux l'égalité demeure.

Preuve : $2 + 2 = 2 + 1 + 1 = 3 + 1 = 4$

Déf. 1 Déf. 2 Déf. 3

Donc, d'après l'axiome : $2 + 2 = 4$. »

A première vue, cette preuve est entièrement construite à partir des définitions et de l'axiome. Et de cet axiome, on pourrait faire encore une définition, comme Leibniz l'a fait lui-même ailleurs . Il semble qu'il ne soit pas requis de rien savoir de plus sur 1, 2, 3, 4 que ce qui est contenu dans les définitions. Un examen plus serré révèle cependant une lacune, dissimulée par l'omission des parenthèses. On devrait écrire plus exactement :

$$2 + 2 = 2 + (1 + 1)$$
$$(2 + 1) + 1 = 3 + 1 = 4.$$

Manque alors la proposition :

$$2 + (1 + 1) = (2 + 1) + 1$$

qui est un cas particulier de

$$a + (b + c) = (a + b) + c.$$

Sous l'hypothèse de cette loi, on voit aisément qu'on peut démontrer toutes les formules de l'addition. Cela revient à définir chaque nombre à partir de son prédécesseur. Et je ne vois pas comment le nombre 437 986 pourrait être donné plus adéquatement qu'en usant du procédé leibnizien. De la sorte, le nombre tombe en notre pouvoir sans que nous en ayons une représentation. Par ces définitions, on peut réduire l'ensemble infini des nombres au nombre 1 et à l'adjonction d'une unité; chacune des formules numériques infiniment nombreuses peut être prouvée à partir de quelques propositions générales.

GIUSEPPE PEANO

(pp. 1-20)

ARITHMETICES PRINCIPIA.

§ 1. De numeris et de additione.

Explicationes.

Signo N significatur *numerus (integer positivus).*
» 1 » *unitas.*
» $a+1$ » *sequens a*, sive *a plus* 1.
» $=$ » *est aequalis.* Hoc ut novum signum considerandum est, etsi logicae signi figuram habeat.

Axiomata.

1. $1 \in N$.
2. $a \in N . \supset . a = a$.
3. $a, b \in N . \supset : a = b . = . b = a$.
4. $a, b, c \in N . \supset \therefore a = b . b = c : \supset . a = c$.
5. $a = b . b \in N : \supset . a \in N$.
6. $a \in N . \supset . a + 1 \in N$.
7. $a, b \in N . \supset : a = b . = . a + 1 = b + 1$.
8. $a \in N . \supset . a + 1 - = 1$.
9. $k \in K \therefore 1 \in k \therefore x \in N . x \in k : \supset_x . x + 1 \in k :: \supset . N \supset k$.

Definitiones.

10. $2 = 1 + 1 ; 3 = 2 + 1 ; 4 = 3 + 1$; etc.

Theoremata.

11. $2 \in N$.

Demonstratio :

P 1 . ⊃ :	$1 \in N$	(1)
1 [a] (P 6) . ⊃ :	$1 \in N . \supset . 1 + 1 \in N$	(2)
(1) (2) . ⊃ :	$1 + 1 \in N$	(3)
P 10 . ⊃ :	$2 = 1 + 1$	(4)
(4) . (3) . (2, 1 + 1) [a, b] (P 5) : ⊃ :	$2 \in N$	(Theorema).

Opere Scelta Edizioni Cremonese Roma 1958. Vol. II, p.34.

Note : voici quelques indications pour " déchiffrer " la page de Peano donnée en illustration.

⊃: signifie implique (⊃ ou ⟹) ; c'est un C retourné première lettre de Consequor.

ε: le signe d'appartenance (∈) ; c'est un epsilon première lettre du verbe être en grec.

−: est le signe de la négation. Donc $- =$ en 8. Veut dire $\neq$.

Les points (. ; : ; ∴) remplacent les parenthèses : ils se mettent autour des opérateurs, et s'accumulent autour de l'opérateur principal.

Texte 16 : Poincaré : le raisonnement par récurrence.

POINCARE : La science et l'hypothèse, 1902.
Flammarion, chapitre I, § V.

Le caractère essentiel du raisonnement par récurrence c'est qu'il contient, condensés pour ainsi dire en une formule unique, une infinité de syllogismes.

Pour qu'on s'en puisse mieux rendre compte, je vais énoncer les uns après les autres ces syllogismes qui sont, si l'on veut me passer l'expression, disposés en cascade.

Ce sont bien entendu des syllogismes hypothétiques.

Le théorème est vrai du nombre 1.

Or s'il est vrai de 1, il est vrai de 2.

Donc il est vrai de 2.

Or s'il est vrai de 2, il est vrai de 3.

Donc il est vrai de 3, et ainsi de suite.

On voit que la conclusion de chaque syllogisme sert de mineure au suivant.

De plus les majeures de tous nos syllogismes peuvent être ramenées à une formule unique.

Si le théorème est vrai de $n - 1$, il l'est de n.

On voit donc que, dans les raisonnements par récurrence, on se borne à énoncer la mineure du premier syllogisme, et la formule générale qui contient comme cas particuliers toutes les majeures.

Cette suite de syllogismes qui ne finirait jamais se trouve ainsi réduite à une phrase de quelques lignes.

Il est facile maintenant de comprendre pourquoi toute conséquence particulière d'un théorème peut, comme je l'ai expliqué plus haut, être vérifiée par des procédés purement analytiques.

Si au lieu de montrer que notre théorème est vrai de tous les nombres, nous voulons seulement faire voir qu'il est vrai du nombre 6 par exemple, il nous suffira d'établir les 5 premiers syllogismes de notre cascade; il nous en faudrait 9 si nous voulions démontrer le théorème pous le nombre 10; il nous en faudrait davantage encore pour un nombre plus grand; mais quelque grand que soit ce nombre nous finirions toujours par l'atteindre, et la vérification analytique serait possible.

Et cependant, quelque loin que nous allions ainsi, nous ne nous élèverions jamais jusqu'au théorème général, applicable à tous les nombres, qui seul peut être objet de science. Pour y arriver, il faudrait une infinité de syllogismes, il faudrait franchir un abîme que la patience de l'analyste, réduit aux seules ressources de la logique formelle, ne parviendra jamais à combler.

Je demandais au début pourquoi on ne saurait concevoir un esprit assez puissant pour apercevoir d'un seul coup d'œil l'ensemble des vérités mathématiques.

La réponse est aisée maintenant; un joueur d'échecs peut combiner quatre coups, cinq coups d'avance, mais, si extraordinaire qu'on le suppose, il n'en préparera jamais qu'un nombre fini; s'il applique ses facultés à l'arithmétique, il ne pourra en apercevoir les vérités générales d'une seule intuition directe; pour parvenir au plus petit théorème, il ne pourra s'affranchir de l'aide du raisonnement par récurrence parce que c'est un instrument qui permet de passer du fini à l'infini.

Cet instrument est toujours utile, puisque, nous faisant franchir d'un bond autant d'étapes que nous le voulons, il nous dispense de vérifications longues, fastidieuses et monotones qui deviendraient rapidement impraticables. Mais il devient indispensable dès qu'on vise au théorème général, dont la vérification analytique nous rapprocherait sans cesse, sans nous permettre de l'atteindre.

Dans ce domaine de l'arithmétique, on peut se croire bien loin de l'analyse infinitésimale, et, cependant, nous venons de le voir, l'idée de l'infini mathématique joue déjà un rôle prépondérant, et sans elle il n'y aurait pas de science parce qu'il n'y aurait rien de général.

Le principe de récurrence dans le traité du triangle arithmétique de Pascal.

Quoique cette proposition ait une infinité de cas, j'en donnerai une démonstration bien courte, en supposant 2 lemmes.

Le 1, qui est évident de soi-même, que cette proportion se rencontre dans la seconde base ...

Le 2, que si cette proportion se trouve dans une base quelconque, elle se trouvera nécessairement dans la base suivante.

D'où il se voit qu'elle est nécessairement dans toutes les bases : car elle est dans la seconde base par le premier lemme; donc par le second elle est dans la troisième base, donc dans la quatrième, et à l'infini.

Il faut donc seulement démontrer le second lemme, en cette sorte.

PASCAL : Traîté du triangle arithmétique

6 - PROBLEMES.

Les mathématiques, ce sont d'abord les problèmes. Et la Théorie des Nombres, c'est justement une source inépuisable de problèmes, petits ou grands, dont l'énoncé le plus simple cache parfois de redoutables difficultés.

Texte 17 : Diophante : un système du second degré.

Commençons par Diophante, le grand ancêtre de notre arithmétique, qui a donné son nom aux équations diophantiennes : celles que l'on doit résoudre en nombres entiers, ou rationnels.

Dans le cas présent, il s'agit de rationnels. En notation actuelle, l'auteur propose de résoudre en nombres rationnels le système :

$$x^2 + y = a^2 \quad , \quad y^2 + x = b^2 \quad .$$

Le " premier nombre " étant x, Diophante suppose que le second y, est égal à 1 + 2x, ce qui conduit à a = x + 1 et transforme la seconde équation en :

$$4x^2 + 5x + 1 = b^2 \quad .$$

Il suppose alors que b = 2x - 2 et cette équation devient alors :

$$4x^2 + 5x + 1 = 4x^2 - 8x + 4 \quad ,$$

ou encore : $13x = 3$,

d'où $x = \frac{3}{13}$ et $y = \frac{19}{13}$.

DIOPHANTE : Livres Arithmétiques. Livre II. Problème 20.
Traduction P. Vereeke.

Trouver deux nombres tels que le carré de chacun d'eux, accru du nombre restant, forme un carré.

Que le premier nombre soit 1 arithme, et le second nombre 1 unité plus 2 arithmes, de manière que le carré du premier nombre, accru du second nombre, forme un carré. Il faut encore que le carré du second nombre, accru du premier nombre, forme aussi un carré. Mais le carré du second nombre, accru du premier nombre forme 4 carrés d'arithme plus 5 arithmes plus 1 unité, ce qui doit être égal à un carré.

Formons le carré de 2 arithmes moins 2 unités ; ce carré sera donc 4 carrés d'arithme plus 4 unités moins 8 arithmes, et l'arithme devient $\frac{3}{13}$. Dès lors, le premier nombre sera $\frac{3}{13}$, le second sera $\frac{19}{13}$, et ces nombres résolvent le problème .

Bien sûr, il ne s'agit que d'une solution. Euler a trouvé la solution générale en posant

$$x^2 + y = (p - x)^2 \quad \text{et} \quad y^2 + x = (q - y)^2 \quad .$$

Le lecteur complétera.

Texte 18 : NICOMAQUE DE GERASE : génération des cubes.

Voici encore un extrait, un peu obscur celui-ci, de Nicomaque de Gérase. Le problème en question est contenu dans le dernier paragraphe : l'auteur traite de la suite des nombres impairs :

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, ...

Le premier, qui est 1, est égal au cube de 1, bien sûr.

Les deux suivants, 3 et 5, ont pour somme 8, cube de 2.

Les trois suivants, 7, 9 et 11, ont pour somme $27 = 3^3$. Et ainsi de suite.

Pouvez-vous le démontrer ?

NICOMAQUE DE GERASE : Introduction arithmétique. IIe siècle après J.-C.
Livre II, chapitre XX § 5. Traduction J.Bertier. Vrin 1978.

Mais ce qui confirmera le mieux que l'*impair* est absolument cause d'*Identité* et jamais le *pair*, il faut le démontrer dans toute ecthèse proportionnelle à partir de l'unité, par exemple *double* :

1, 2, 4, 8, 16, 32, 64, 128, 256,

triple :

1, 3, 9, 27, 81, 243, 729, 2187,

et jusqu'où tu veux ; tu trouveras que nécessairement tous les termes dans les champs *impairs* sont *carrés*, mais autres, jamais en aucune façon, et qu'aucun n'est *carré* dans un champ *pair* ; et tous les nombres ur nombre de fois égal égaux un nombre de fois égal, c'est-à-dire les cubes qui sont étendus en *trois* dimensions et qui semblent participer encore plus à l'*Identité*, sont l'oeuvre des *impairs* et non pas des *pairs* :

1, 8, 27, 64, 125 et 216

et ceux qui progressent selon la même loi par un procédé simple et invariable ; car, une fois exposés les *impairs* successifs à partir de l'unité et à l'infini, observe ceci : le premier produit le cube en puissance, les deux qui viennent après lui, réunis, produisent le second, les trois qui viennent après eux produisent le troisième, les quatre qui succèdent à ceux-là, produisent le quatrième, les cinq suivants produisent le cinquième, les six suivants, le sixième, et cela toujours.

Note : ecthèse : terme d'une progression.

Texte 19 : Bachet : un problème plaisant du premier degré.

Claude-Gaspar BACHET, sieur de Mériziac, est en fait le véritable inventeur du théorème dit identité de Bezout. C'est Bachet qui dans son ouvrage " Problèmes plaisants et délectables qui se font par les nombres " (édition de 1624) a présenté pour la première fois la solution de l'équation en nombres entiers ax + by = c.

Voici un exemple de ces " problèmes plaisants ", qui fait justement intervenir cette sorte d'équation (sachez qu'un sou vaut 12 deniers).

BACHET : Problèmes plaisants et délectables qui se font par les nombres. 1624.

X

Il y a 41 personnes en un banquet tant hommes que femmes et enfants qui en tout dependent 40 sous, mais chaque homme paye 4 sous, chaque femme 3 sous, chaque enfant ¼ deniers. Je demande combien il y a d'hommes, combien de femmes, combien d'enfants.

Texte 20 : FERMAT : un testament.

Le véritable seigneur des problèmes d'arithmétique, c'est bien sûr Pierre de Fermat. Comme nous l'avons vu, son oeuvre ne comporte nul traité, mais des lettres à d'autres savants de son époque, qui contiennent des défis et des réultats.

Voici un extrait d'une lettre à Carcavi, d'août 1659, que Jean Itard a qualifié de testament de Fermat en matière de Théorie des Nombres. Notre auteur y consigne un grand nombre de résultats trouvés ou conjecturés par lui, les exprimant sous une forme qui appelle quelques explications.

Il commence par la propriété déjà vue plus haut (Texte n°11) et sur laquelle nous ne reviendrons pas.

Puis, un théorème qui est peut-être le plus beau de ceux qui furent formulés à cette époque : tout nombre premier de la forme 4k + 1 est somme de deux carrés. Par exemple $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, etc... On pourrait ajouter que cette décomposition est unique et qu'aucun entier de la forme 4k - 1 n'est somme de deux carrés.

Ensuite, un résultat intéressant par sa généralité : tout entier naturel est somme de quatre carrés, certains pouvant être nuls.

La question suivante pose un problème de paternité : il s'agit de l'équation : $ax^2 = y^2 - 1$ (ou $ax^2 = y^2 + 1$) que les auteurs anglo-saxons, et même certains français, nomment équation de Pell, et qu'il faudrait appeler équation de Fermat, puisque celui-ci a proclamé plusieurs fois que cette équation admet une infinité de solutions entières dès lors que l'entier naturel a n'est pas un carré.

" Il n'y a aucun cube divisible en deux cubes " traduit le fait que l'équation $x^3 + y^3 = z^3$ n'admet aucune solution en nombres entiers (ou rationnels) autre que les " triviales " $0^3 + 0^3 = 0^3$ et $0^3 + 1^3 = 1^3$.
On sait que Fermat a affirmé par ailleurs qu'il en était de même pour l'équation $x^n + y^n = z^n$ avec $n \geqslant 3$, mais que ce " grand théorème " n'est toujours pas démontré, même si l'on sait depuis 1983, depuis la démonstration par Gerd Faltings d'une conjecture de Mordell de 1922, que cette équation n'a qu'un nombre fini de solutions.

Les deux assertions suivantes portent sur les équations diophantiennes $x^2 + 2 = y^3$ et $x^2 + 4 = y^3$, à résoudre en nombres entiers. Les affirmations de Fermat sont exactes, mais il paraît difficile de les démontrer en se bornant à des considérations telles que la descente infinie, qui ne sort pas du cadre des nombres entiers naturels. Il faut recourir à l'arithmétique complexe créée par Gauss, qui permet de factoriser $x^2 + 2$ et $x^2 + 4$.

Tout grand homme a ses points faibles, et ce qui suit va encore le montrer. Quand il parle des " puissances carrées de 2 ", Fermat envisage les nombres qui se déduisent de 2 par une suite d'élévations au carré : il affirme donc que tous les nombres de la forme $\mathcal{F}_n = 2^{2^n} + 1$ sont premiers. En effet, $\mathcal{F}_0 = 3$, $\mathcal{F}_1 = 5$, $\mathcal{F}_2 = 17$, $\mathcal{F}_3 = 257$ $\mathcal{F}_4 = 65537$ sont premiers, mais Fermat n'a pas vu que $\mathcal{F}_5$, qui s'écrit avec dix chiffres dans le système décimal, est composé : Euler a prouvé en 1732 que $\mathcal{F}_5$ est divisible par 641. A vrai dire, $\mathcal{F}_n$ est composé pour tous les n tels que $5 \leqslant n \leqslant 19$, et pour d'autres valeurs de n. Selon l'opinion la plus répandue aujourd'hui, l'ensemble des nombres $\mathcal{F}_n$ premiers est fini, mais on ne sait pas le démontrer.

La suite du texte se comprend aisément : elle concerne l'équation diophantienne $(2x^2 - 1)^2 = 2y^2 - 1$, qui a pour seules solutions entières $x = 1$ et $x = 2$, mais ceci n'a été démontré qu'en 1883 par Genocchi. Puis encore quelques diophantiennes, et le tout se termine par une question sur les nombres polygones, un sujet dont l'étude remonte à l'Antiquité (voir texte n°3 § 3).

FERMAT : Lettre à Carcavi - Août 1659.

... Pour ce que les méthodes ordinaires, qui sont dans les livres, étaient insuffisantes à démontrer des propositions si difficiles, je trouvai enfin une route tout à fait singulière pour y parvenir.

J'appelai cette manière de démontrer la *descente infinie* ou *indéfinie* ; je ne m'en servis au commencement que pour démontrer les propositions négatives, comme, par exemple :

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

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

La preuve se fait par réduction à l'absurde en cette manière :

S'il y avait aucun triangle rectangle en nombres entiers qui eût son aire égale à un carré, il y aurait un autre triangle moindre que celui-là qui aurait la même propriété. S'il y en avait un second, moindre que le premier, qui eût la même propriété, il y en aurait, par un pareil raisonnement, un troisième, moindre que ce second, qui aurait la même propriété, et enfin un quatrième, un cinquième, à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends parler toujours des nombres entiers). D'où on conclut qu'il est donc impossible qu'il y ait aucun triangle rectangle dont l'aire soit carrée.

On infère de là qu'il n'y en a non plus en fractions dont l'aire soit carrée ; car, s'il y en avait en fractions, il y en aurait en nombres entiers, ce qui ne peut pas être, comme il se peut prouver par la descente.

Je n'ajoute pas la raison d'où j'infère que, s'il y avait un triangle rectangle de cette nature, il y en aurait un autre de même nature moindre que le premier, parce que le discours en serait trop long et que c'est là tout le mystère de ma méthode. Je serai bien aise que les Pascal et les Roberval et tant d'autres savants la cherchent sur mon indication.

Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que lorsqu'il me fallut démontrer que *tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux carrés*, je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquaient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité. Ce progrès de mon raisonnement en ces questions affirmatives est tel : si un nombre premier pris à discrétion, qui surpasse de l'unité un multiple de 4, n'est point composé de deux carrés, il y aura un nombre premier de même nature, moindre que le donné, et ensuite un troisième encore moindre, etc., en descendant à l'infini jusques à ce que vous arriviez au nombre 5, qui est le moindre de tous ceux de cette nature, lequel il s'ensuivrait n'être pas composé de deux carrés, ce qu'il est pourtant. D'où on doit inférer, par la déduction à l'impossible, que tous ceux de cette nature sont, par conséquent, composés de deux carrés.

Il y a infinies questions de cette espèce, mais il y en a quelques autres qui demandent des nouveaux principes pour y appliquer la *descente*, et la recherche en est quelquefois si malaisée qu'on n'y peut venir qu'avec une peine extrême. Telle est la question suivante que Bachet sur Diophante avoue n'avoir jamais pu démontrer, sur le sujet de laquelle M. Descartes fait dans une de ses lettres la même déclaration, jusque-là qu'il confesse qu'il la juge si difficile qu'il ne voit point de voie pour la résoudre.

Tout nombre est carré ou composé de deux, de trois ou de quatre carrés.

Je l'ai enfin rangée sous ma méthode et je démontre que, si un nombre donné n'était point de cette nature, il y en aurait un moindre qui ne le serait pas non plus, puis un troisième moindre que le second, etc., à l'infini ; d'où l'on infère que tous les nombres sont de cette nature.

Celle que j'avais proposée à M. Frenicle et autres est d'aussi grande ou même plus grande difficulté : Tout nombre non carré est de telle nature qu'il y a infinis carrés qui, multipliant ledit nombre, font un carré moins 1. Je la démontre par la *descente* appliquée d'une manière toute particulière.

J'avoue que M. Frenicle a donné diverses solutions particulières et M. Wallis aussi, mais la démonstration générale se trouvera par la *descente* dûment et proprement appliquée : ce que je leur indique, afin qu'ils ajoutent la démonstration et construction générale du théorème et du problème aux solutions singulières qu'ils ont données.

J'ai ensuite considéré certaines questions qui, bien que négatives, ne restent de recevoir très grande difficulté, la méthode pour y pratiquer la *descente* étant tout à fait diverse des précédentes, comme il sera aisé d'éprouver. Telles sont les suivantes :

Il n'y a aucun cube divisible en deux cubes.

Il n'y a qu'un seul carré en entiers qui, augmenté du binaire, fasse un cube. Le dit carré est 25.

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

Toutes les puissances carrées de 2, augmentées de l'unité, sont nombres premiers.

Cette dernière question est d'une très subtile et très ingénieuse recherche et, bien qu'elle soit conçue affirmativement, elle est négative, puisque dire qu'un nombre est premier, c'est dire qu'il ne peut être divisé par aucun nombre.

Je mets en cet endroit la question suivante dont j'ai envoyé la démonstration à M. Frenicle, après qu'il m'a avoué et qu'il a même témoigné dans son Ecrit imprimé qu'il n'a pu la trouver :

Il n'y a que les deux nombres 1 et 7 qui, étant moindres de l'unité qu'un double carré, fassent un carré de même nature, c'est-à-dire qui soit moindre de l'unité qu'un double carré.

Après avoir couru toutes ces questions, la plupart de diverse nature et de différente façon de démontrer, j'ai passé à l'invention des règles générales pour résoudre les équations simples et doubles du Diophante.

On propose, par exemple,

2 Q + 7967 égaux à un carré

J'ai une règle générale pour résoudre cette équation, si elle est possible, ou découvrir son impossibilité, et ainsi en tous les cas et en tous nombres tant des carrés que des unités.

On propose cette équation double :

2 N + 3 et 2 N + 5 égaux chacun à un carré

Bachet se glorifie, en ses Commentaires sur Diophante, d'avoir trouvé une règle en deux cas particuliers ; je la donne générale en toute sorte de cas et détermine par règle si elle est possible ou non.

J'ai ensuite rétabli la plupart des propositions défectueuses de Diophante et j'ai fait celles que Bachet avoue ne savoir pas et la plupart de celles auxquelles il paraît que Diophante même a héaité, dont je donnerai des preuves et des exemples à mon premier loisir.

J'avoue que mon invention pour découvrir si un nombre donné est premier ou non n'est pas parfaite, mais j'ai beaucoup de voies et de méthodes pour réduire le nombre des divisions et pour les diminuer beaucoup en abrégeant le travail ordinaire. Si M. Frenicle baille ce qu'il a médité là-dessus, j'estime que ce sera un secours très considérable pour les savants.

La question qui m'a occupé sans que j'aie encore pu trouver aucune solution est la suivante, qui est la dernière du livre de Diophante *Des nombres polygones* :

Trouver de combien de manières un nombre donné peut être polygone.

Le texte de Diophante étant corrompu, nous ne pouvons pas deviner sa méthode ; celle de Bachet ne m'agrée pas et elle est trop difficile aux grands nombres. J'en ai bien trouvé une meilleure, mais elle ne me satisfait pas encore.

Il faut chercher en suite de cette proposition la solution du problème suivant :

Trouver un nombre qui soit polygone autant de fois et non plus qu'on voudra, et trouver le plus petit de ceux qui satisfont à la question.

Voilà sommairement le compte de mes rêveries sur le sujet des nombres. Je ne l'ai écrit que parce que j'appréhende que le loisir d'étendre et de mettre au long toutes ces démonstrations et ces méthodes me manquera ; en tout cas, cette indication servira aux savants pour trouver d'eux-mêmes ce que je n'étends point, principalement si MM. de Carcavi et Frenicle leur font part de quelques démonstrations *par la descente* que je leur ai envoyées sur le sujet de quelques propositions négatives. Et peut-être la postérité me saura gré de lui avoir fait connaître que les Anciens n'ont pas tout su, et cette relation pourra passer dans l'esprit de ceux qui viendront après moi pour *traditio lampadis ad filios*,(1) comme parle le grand Chancelier d'Angleterre, suivant le sentiment et la devise duquel j'ajouterai :

Multi pertransibunt et augebitur scientia.(2)

(1) La transmission du flambeau aux générations suivantes.

(2) Beaucoup iront au delà et la science sera augmenté.

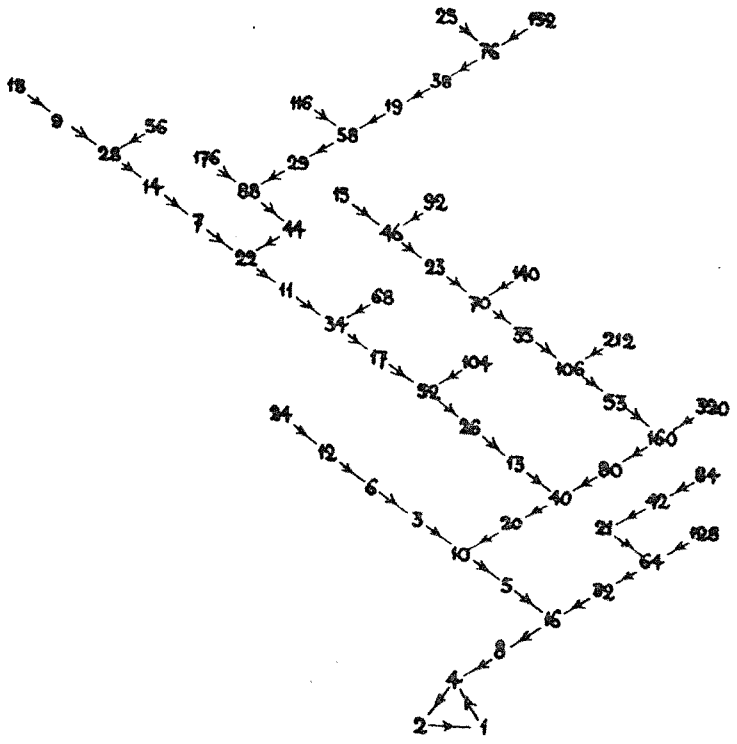
Note : N désigne chez Bachet, le nombre inconnu et Q son carré.

Texte 21 : Collatz : le problème de Syracuse.

Contrairement à une opinion répandue, les mathématiques ne sont par arrêtées, elles comportent encore bien des problèmes ouverts, que nul ne sait résoudre. Leurénoncé est parfois fort simple. En voici un exemple, connu sous le nom de " Problème de Syracuse ".

Quand il était étudiant, L. Collatz demanda si la suite définie par : $a_{n+1} = a_n/2$ (a_n pair), $a_{n+1} = 3a_n + 1$ (a_n impair) a une structure d'arbre, mis à part le cycle 4, 2, 1, 4, ... (voir figure), c'est-à-dire que, partant d'un entier positif a_1, il existe une valeur de n pour laquelle $a_n = 1$. Ceci a été vérifié pour tous les entiers a_1 inférieurs à 10^9 par D.H. et Emma Lehmer et J.-L. Selfridge, et par d'autres jusqu'à 7×10^{11}.

RICHARD K. GUY : Unsolved problems in Number Theory (1981).



7 - POUR EN SAVOIR PLUS.

En général.

1) Arithmétique et théorie des nombres, J. Itard.
   Que sais-je ? n° 1093.
2) Les nombres et leurs sytèmes, A. Warusfel.
   Points Sciences S 21, Seuil.
3) Les nombres remarquables, F. Le Lionnais.
   Hermann (Anatolius revu et augmenté !).

Sur les nombres premiers.

4) Les nombres premiers, J. Itard.
   Que sais-je ? n° 571.
5) A nous les grands nombres premiers, H. Cohen.
   dans La Recherche n° 135, juillet-août 1982.
   (Nouveaux algorithmes pour calculer des nombres premiers à l'aide de l'informatique.)
6) Cryptographie publique, A. Bouvier.
   dans Bulletin de l'APMEP n° 336, décembre 1982.

Sur les nombres décimaux.

7) Vers une épistémologie des décimaux, M. Abdeljaouad.
   dans Fragments d'histoire des mathématiques, brochure APMEP n° 41.
8) Introduction du calcul décimal et du sytème métrique dans la région de Rouen pendant la Révolution.
   IREM de Rouen, juin 1979 et la Rigueur et le Calcul, CEDI 1982.

Sur le grand théorème de Fermat.

9) Historique du dernier théorème de Fermat, P. Ribenboim.
   dans Fragments d'histoire des mathématiques.
   Brochure APMEP n° 41.
10) Le grand théorème de Fermat, H. Edwards.
   dans Pour La Science n° 14, décembre 1978.
   Une enigme mathématique : le dernier théorème de Fermat, Th. Got.
   dans Les Grands Courants de la Pensée Mathématique. Le Lionnais, Blanchard 1762.

Sur la loi de réciprocité quadratique.

11) Histoire d'un théorème d'arithmétique : la loi de réciprocité quadratique, R. Cuculière. IREM de Paris-Nord, 1980.

Sur les nombres transcendants.

12) Les victoires de la transcendance par M. Waldschmitt et J. Vélu.
   dans La Recherche n° 84, décembre 1977 (sur les traces de Diophante).

ARITHMETIQUE.

LISTE DES NOMS CITES . (Une étoile figure à côté de ceux pour lesquels figure un texte, un extrait, ou une illustration ; les autres noms figurent dans les commentaires ou dans les textes eux-mêmes.)

Al Kasi
* Anatolius
* Bachet
Bezout
Boèce
Bonfils
Carcavi
* Collatz
* Diophante
Erathostène
* Euclide
Euler
* Fermat
* Frege
Frenicle
* Gauss
Genocchi
Girard
(Guerd Falting)
(Guy)
Hankel
(Itard)
Kant
* Legendre
(Lehmer)
* Leibniz
Mordell
* Nicomaque
* Pascal
* Peano
Pell
* Poincaré
Pythagore
Roberval
(Selfridge)
* Stevin
Viète

BIOGRAPHIES.

ANATOLIUS D'ALEXANDRIE.(IIIè siècle après J.C.)

Philosophe converti au christianisme. Ecrivit notamment une Introduction à l'Arithmétique, aujourd'hui perdue. Il nous reste de lui divers fragments sur les nombres, surtout ce qui est cité dans un livre du Pseudo-Jamblique. Ces textes sont intéressants comme témoignage sur l'arithmologie des Anciens ; il est difficile de savoir ce qui remonte véritablement aux Pythagoriciens ou à Pythagore lui-même, qui vivaient sept ou huit siècles plus tôt, et sur lesquels nous n'avons que des informations très indirectes et très pauvres, dans des textes tardifs, et composites (cf. Walter BURKERT, Lere and Science in ancient Pythagoreanism, Harvard U.P. 1972).

NICOMAQUE DE GERASE. (IIe siècle après J.-C.).

Originaire de Gérase, ville de Palestine, il a dû mourir en 196 après J.-C.. Il était connu pour ses talents d'arithméticien et son oeuvre se situe aux confins de la philosophie et des sciences. Ses oeuvres écrites en grec ont été traduites et commentées en latin et en arabe ce qui leur a assuré une grande diffusion.

FREGE Goltlob. (1848 - 1925).

Mathématicien et logicien Allemand. Né à Wismar, professeur à Iéna, il a surtout travaillé sur les fondements de l'arithmétique et a crée un langage formalisé, origine d'autres travaux sur la logique formelle dont il est un des précurseurs.

PEANO Giuseppe. (1858 - 1932).

Mathématicien et logicien italien. Né à Cuno, professeur à Turin, il a surtout travaillé sur le calcul différentiel et intégral, les fondements des mathématiques, et la linguistique. Dans ces trois domaines, il est resté célébre par l'exemple d'une courbe qui remplit toute l'aire d'un carré, une axiomatique de $\mathbb{N}$, la création d'une langue internationale : l'Interlingua.

POINCARE Jules Henri. (1854 - 1912).

Mathématicien et savant français. Né à Nancy, il fut sans doute le mathématicien le plus célébre du début du XXe siècle et un savant universel dont l'oeuvre est importante dans de nombreux domaines des mathématiques, mais aussi en mécanique, astronomie, physique mathématique et philosophie des sciences. Ses ouvrages dans ce dernier domaine sont facilement accessibles. Il fut aussi un précurseur de l' intuitionnisme.