IREM

des Pays de la Loire

LES MATHÉMATIQUES NE SE SONT PAS FAITES EN UN JOUR ...

Promenades historiques

Troisième promenade : Au pays de l'arithmétique.

Mars 2001

INSTITUT DE RECHERCHE SUR
L'ENSEIGNEMENT DES MATHÉMATIQUES
DES PAYS DE LA LOIRE

2, rue de la Houssinière • BP 92208
44322 NANTES CEDEX 03
Tel. 02 51 12 59 41
Site : www.irem.sciences.univ-nantes.fr/

PREAMBULE

Nous vous proposons au travers d'une série de petits cahiers quelques promenades historiques au fil des mathématiques.

Nous nous adressons autant aux élèves qu'aux professeurs ; chacun, nous l'espérons pourra y trouver son compte.

Pour cela, nous avons choisi un langage simple et vous trouverez au long des pages des activités expérimentées par nos élèves. Ces activités permettent soit d'introduire une notion du programme, soit de la prolonger, soit aussi d'acquérir une "culture" mathématique.

Les mathématiques ne se sont pas faites en un jour ; elles continuent de se construire. Elles ont une histoire pleine de bonds et de rebonds. En lisant cette histoire, l'élève comprendra que ses difficultés furent peut-être aussi celles des plus grands mathématiciens. Il découvrira comment certaines notions ont évolué et pourquoi. Il fera des mathématiques autrement.

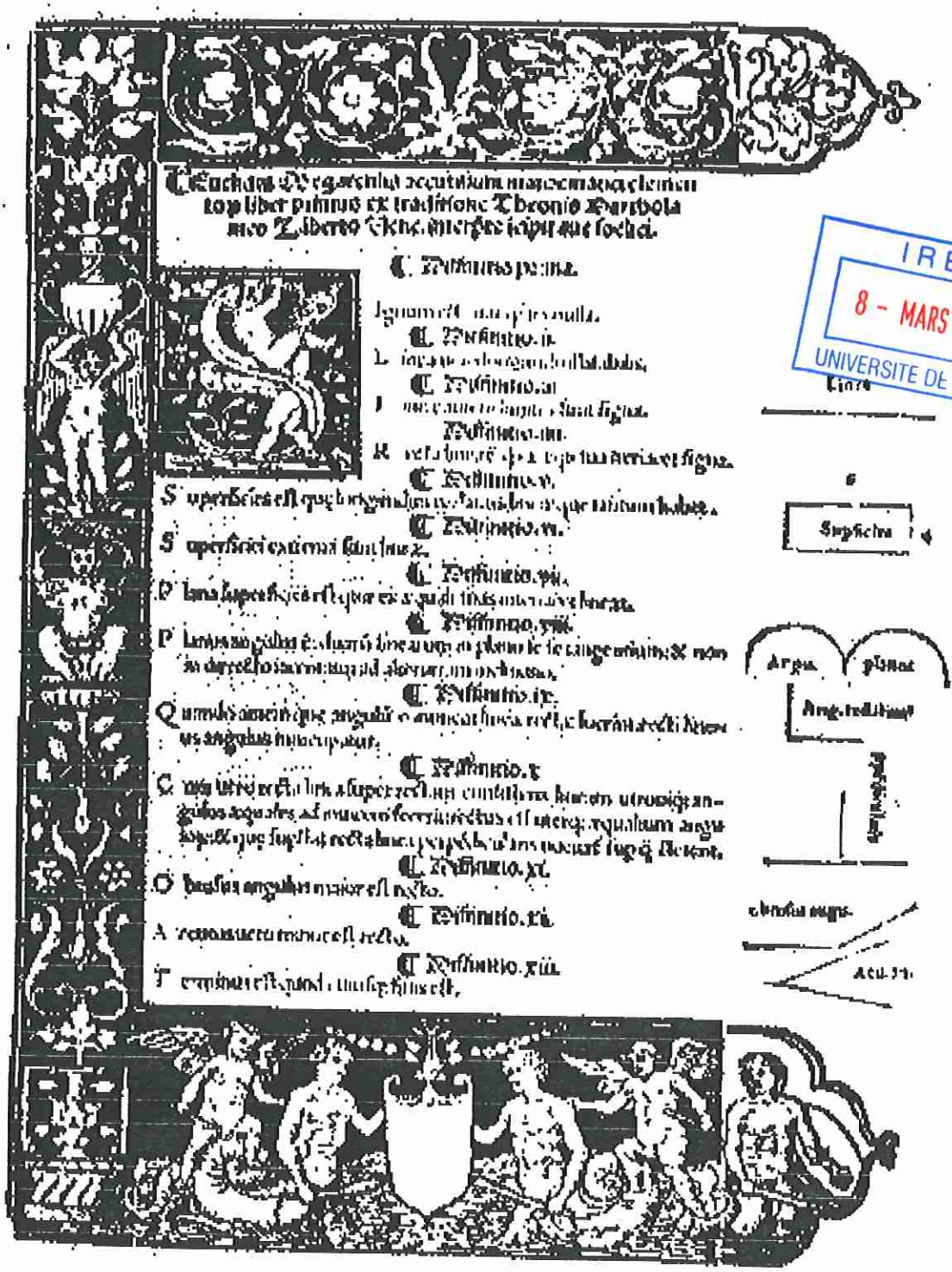
Nous appuierons ces promenades sur la lecture de textes originaux en proposant, lorsque cela semble nécessaire pour la compréhension, des traductions en termes plus modernes.

Nous indiquerons les niveaux d'accessibilité, et les prérequis, le cas échéant. Mais nous avons pris le parti de ne privilégier aucun niveau, du collège au lycée, en passant par le lycée professionnel.

Nous vous souhaitons d'agréables promenades mathématiques; le rêve est peut-être au bout du chemin.

Ce fascicule s'adresse plutôt à des élèves de terminale.
Néanmoins, les chapitres sur l'algorithme d'Euclide et sur les nombres premiers peuvent être abordés par des élèves de seconde, en thèmes d'études par exemple.
Le chapitre sur les nombres premiers, en particulier, peut se lire sans arrière pensée mathématique, juste pour le plaisir de l'étonnement.

Les auteurs de ce fascicule, **Marie-Céline Comairas et Anne Boyé** remercient pour leur contribution Jean Pézennec, Bernard Truffault et Xavier Lefort.



Eléments d'Euclide : première traduction directement à partir du texte grec. Edition de 1505.

1 - L'algorithme d'Euclide

1 Voici quelques définitions que l'on peut lire au début du livre VII des Eléments d'Euclide[1] :

1. L'unité est ce suivant quoi chacune des choses existantes est dite une.
2. Le nombre est une multitude composée d'unités.
3. Un nombre est une partie d'un nombre, le plus petit du plus grand, lorsqu'il mesure le plus grand.
4. Mais il est plusieurs parties lorsqu'il ne le mesure pas.
5. Un plus grand nombre est multiple d'un plus petit lorsqu'il est mesuré par le plus petit.
11. Le nombre premier est celui qui est mesuré par la seule unité.
12. Les nombres premiers entre eux sont ceux qui sont mesurés par la seule unité comme seule commune mesure.

Question 1 : A la lecture de ces définitions, 1 est-il un nombre pour Euclide ?

Question 2 : Traduire le mot « mesurer » dans le langage d'aujourd'hui.

Question 3 : En utilisant la définition 3, nous pourrions écrire que 7 est une partie de 21, car 7 vaut un tiers de 21.

Par contre, en utilisant la définition 4, 14 est « plusieurs parties » de 21, pourquoi ?

Traduire ces deux affirmations avec le langage d'aujourd'hui. [2]

Question 4 : Que signifie qu'un nombre est multiple d'un autre ? Donner un exemple.

---

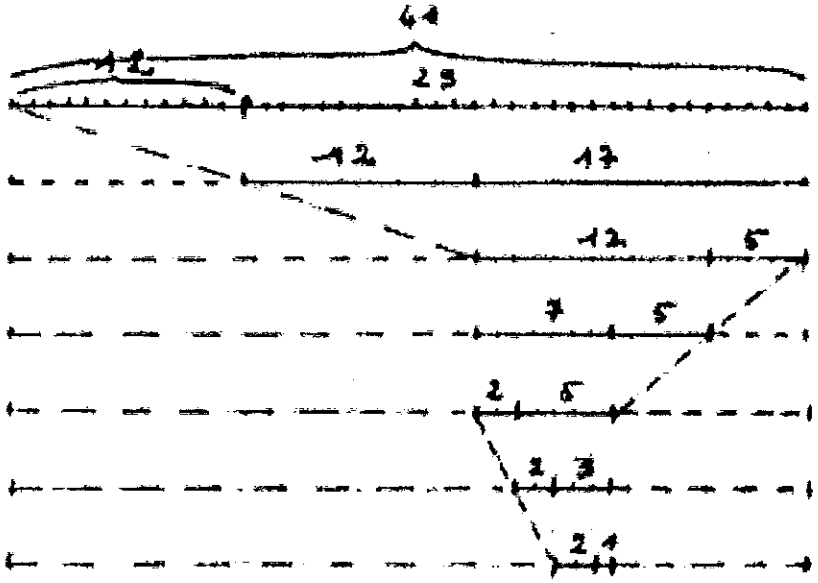
[1] La traduction des Eléments d'Euclide utilisée ici est celle proposée par J. Itard, *Les livres arithmétiques d'Euclide*, 1961.

[2] Les mots "numérateur" et "dénominateur" trouvent leur origine dans des considérations de ce genre. Par exemple si l'on considère la fraction $\frac{2}{3}$, c'est à dire deux tiers, cela signifie que l'on a pris deux parties qui se nomment des tiers. Le dénominateur indique le nom des parties que l'on prend, il dénomme ; le numérateur indique le nombre de parties que l'on prend, il « numère ».

2 a) Voici deux nombres entiers : 41 et 12, et voici une liste d'opérations réitérées :

Plus grand	Plus petit	Plus grand - plus petit	Remarques
41	12	29	
29	12	17	
17	12	5	$41 = 3 \times 12 + 5$
12	5	7	
7	5	2	$12 = 2 \times 5 + 2$
5	2	3	$5 = 2 \times 2 + 1$
3	2	1	

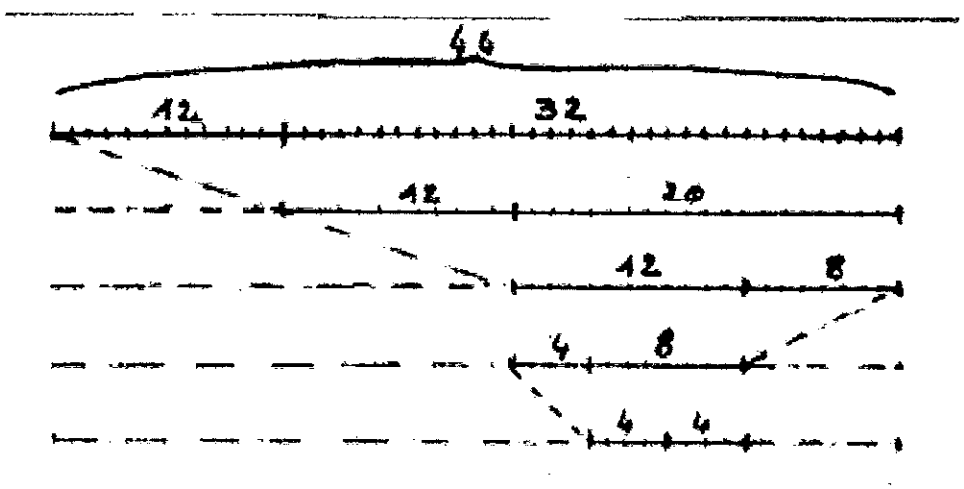
1 « mesure » 41 et 12, et aucun autre nombre qui n'est pas l'unité ne mesure à la fois 41 et 12.



b) Voici un autre exemple :

Plus grand	Plus petit	Plus grand - plus petit	Remarques
44	12	32	
32	12	20	
20	12	8	$44 = 3 \times 12 + 8$
12	8	4	$12 = 1 \times 8 + 4$
8	4	4	$8 = 2 \times 4$

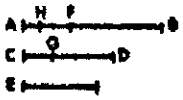
4 « mesure » 44 et 12 ; c'est la plus grande mesure commune possible de 4 et 12.



3 Voici les deux premières propositions du livre VII des éléments d'Euclide :

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 que l'unité, les nombres originaires sont premiers entre eux.



Soient deux nombres AB et CD ; que le plus petit étant continuellement soustrait du plus grand, le reste ne mesure jamais le nombre qui est avant lui jusqu'à ce qu'il reste l'unité ; je dis que AB, CD sont premiers entre eux, c'est à dire que l'unité seule les mesure.

Car si AB et CD ne sont pas premiers entre eux, quelque nombre 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 CG plus petit que lui, et que GC, mesurant FH, laisse l'unité AH.

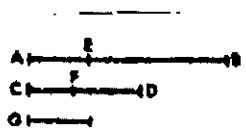
Puisque E mesure CD et que CD mesure BF, E mesure aussi BF. Mais il mesure aussi le tout BA ; donc il mesure le reste AF. Mais AF mesure DG ; donc E mesure aussi DG. Mais il mesure le tout DC ; donc il mesure le reste CG. Mais CG mesure FH ; donc E mesure aussi FH. Mais il mesure le tout FA ; donc il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

Donc aucun nombre ne mesurera les nombres AB et CD ; donc AB, CD sont premiers entre eux.

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 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 quelque 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 FC 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.

Question 1 :

En vous appuyant sur les deux exemples analysés ci-dessus, essayez de comprendre ces deux propositions.

(Note : il sera bon de remarquer que si un nombre r divise a et divise b, alors il divise aussi a - bq, quel que soit q dans N.)

Question 2 :

Ainsi, en prenant deux nombres entiers et en retranchant toujours « le plus petit du plus grand », deux situations peuvent se présenter :

- le dernier reste est 1 ; et 1 est la seule commune mesure aux deux entiers ; ils sont dits alors premiers entre eux.
- le dernier reste est supérieur à 1 ; c'est la plus grande commune mesure aux deux entiers proposés.

Pourquoi Euclide différencie-t-il ces deux cas ?

Question 3 :

Reprenons la proposition 2. Appelons A et B les deux nombres proposés, R_1 le premier reste obtenu après avoir retranché autant de fois que possible (on précisera ce terme), B de A, R_2 le deuxième reste obtenu après avoir retranché autant de fois que possible R_1 de B, etc...

Transcrire en langage d'aujourd'hui cette proposition 2.

Dans le langage actuel, on appelle PGCD de deux entiers a et b leur plus grand diviseur commun (PGCD = Plus Grand Commun Diviseur). Dans le cas où le PGCD de a et b est différent de 1, quel nom Euclide donne-t-il à ce PGCD ?

Comment Euclide exprime-t-il le fait que le PGCD de a et b est 1 ?

Question 4 :

Déterminer, à l'aide de la transcription précédente le PGCD de 285 et 1463 ; puis le PGCD de 42 et 65.

4 L'algorithme d'Euclide :

Le procédé ainsi mis en place permet de déterminer le PGCD de deux nombres entiers a et b. Il est appelé Algorithme d'Euclide.[3]

Si a et b sont deux entiers non nuls tels que $a < b$, il existe un couple unique (q_1, r_1) tel que :

[3] Le mot Algorithme dérive du nom du mathématicien arabe al-Kwarismi (9° siècle ap. J. C.), dont le livre d'arithmétique fut traduit en latin sous le titre : Liber Algorism (livre d'al-Kwarismi) ; le mot algorism fut alors employé pour tout procédé de calcul concernant les chiffres arabes. L'arithmétique elle-même fut parfois appelée algorism. Le mot algorithme est né, sans doute, d'une fusion des deux mots algorism et arithmétique. (Certains dictionnaires anciens donnent comme définition du mot algorism « le système de numération décimal ou arabe »).

De nos jours, on peut trouver dans les dictionnaires d'usage courant la définition suivante du mot algorithme : règles opératoires permettant de résoudre un certain nombre de problèmes. Dans un dictionnaire plus scientifique : ensemble des instructions pouvant être exécutées de façon mécanique pour résoudre une certaine classe de problèmes.

$a = bq_1 + r_1 \qquad 0 \leq r_1 < b;$

C'est la « division euclidienne » de a par b.

Continuons les divisions successives :

$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1.$

....

Les couples $(q_1; r_1)$, $(q_2 ; r_2)$ existent et sont uniques.

Question 1 :

Pourquoi, de façon certaine, la suite des divisions euclidiennes donnera, à une étape (qui sera donc la dernière), un reste nul ?

Question 2 :

Si r_n est le dernier reste non nul, nous avons :

$a = bq_1 + r_1 \qquad 0 \leq r_1 < b$

$b = r_1 q_2 + r_2 \qquad 0 \leq r_2 < r_1$

$r_1 = r_2 q_3 + r_3 \qquad 0 \leq r_3 < r_2$

.....

$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \leq r_n < r_{n-1}$

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

Expliquer pourquoi $D(a , b) = D(b , r_1) = D(r_1, r_2) =$ .....$= D(r_{n-1} , r_n) = D(r_n)$, en désignant par D(a , b) l'ensemble des diviseurs communs à a et b, et $D(r_n)$ l'ensemble des diviseurs de r_n.

Question 3 :

Justifier alors que r_n est le plus grand diviseur commun de a et b.

Exercice :

Déterminer le PGCD de 1100005423 et de 1100000077.

(Note : l'efficacité apparaîtra surtout si on peut comparer l'algorithme d'Euclide à d'autres procédés comme par exemple la décomposition en produit de facteurs premiers.)

L'algorithme d'Euclide vous semble-t-il efficace ?

Le mot algorithme est donc associé à Euclide sans qu'il n'y ait aucun lien de fait entre ces deux noms.

2- Les nombres premiers

I. L'infinité des nombres premiers

Les "nombres premiers" sont un peu comme les "éléments" en chimie ; ils permettent de construire tous les autres nombres entiers. "Premiers", donc les plus simples de tous les nombres, ils sont cependant très étranges. Ils ont fasciné les mathématiciens anciens ... ils fascinent toujours les mathématiciens contemporains, qui, armés de leurs super puissants ordinateurs traquent les "Titans", ces nombres premiers si grands qu'ils ne peuvent même plus être écrits, sinon pensés.

Les nombres premiers sont en effet en nombre infini, contrairement aux éléments de chimie.

Une des plus anciennes preuves de l'infinité des nombres premiers se trouve dans les Éléments d'Euclide, livre IX, proposition 20.

Nous rappelons que dans le livre VII a été défini ce que l'on nomme nombre premier.

Définition 11 : Le nombre premier est celui qui est mesuré par la seule unité.

Ce qui le différencie d'un nombre composé.

Définition 13 : Le nombre composé est celui qui est mesuré par quelque nombre.

Nous rappelons aussi ce que nous avons évoqué lors de l'étude de ce que nous nommons maintenant l'Algorithme d'Euclide :

* 1 n'est pas considéré , en général, comme un nombre dans les Éléments.

* "Un nombre a mesure un nombre b" pourrait être traduit dans notre langage contemporain par "a est un diviseur de b", c'est à dire : "il existe un nombre entier q tel que a = bq".

Question 1 : la définition actuelle d'un nombre premier est -elle exactement celle donnée par Euclide ? Pourquoi ?

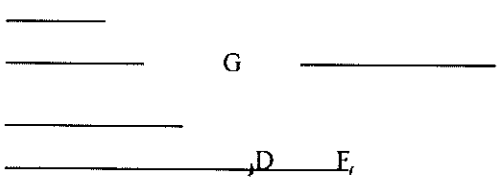
Comment démontrer qu'il existe une infinité de nombres premiers ?

La proposition 20 du livre IX des Éléments d'Euclide :

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.

Voici la démonstration proposée par Euclide:

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 qui est un nombre mesurera le reste, l'unité DF, 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.

Question 2 :

a) Comment appelle-t-on "le plus petit nombre mesuré par A, B, C".?

b) Comment peut-on écrire EF avec les symboles d'opérations actuels ?

c) Préciser pourquoi, si EF n'est pas premier alors il est mesuré par quelque nombre premier. Quel théorème peut-on citer ?

d) Ecrire la fin de la démonstration avec des mots mathématiques actuels. (En particulier, bien noter ce que signifie : G est un nombre.)

e) A votre avis, Euclide a-t-il démontré que l'ensemble des nombres premiers est infini ? Pourquoi Euclide n'utilise pas ce mot "infini" ?

Question 3 : une démonstration contemporaine.

Considérons tous les nombres premiers de 2 à p : 2, 3, 5, 7, …, p.

Soit N le nombre $N = (2\times 3\times 5\times 7\times ...\times p)+1$.

Si N est premier, il existe un nombre premier plus grand que p.

Si N n'est pas premier, démontrer qu'il possède un diviseur premier qui ne fait pas partie de la liste {2, 3, 5, 7, …, p}, donc plus grand que p.

Ainsi, quel que soit le nombre premier p, il existe un nombre premier plus grand que p.

Question 4 : une variante

Pour démontrer que l'ensemble des nombres premiers est infini, on peut démontrer que, quel que soit n entier, il existe toujours un nombre premier plus grand que n.

Pour cela, considérer le nombre N = n! + 1, et faire une démonstration du même type que la précédente.

Euclide

Combien y a-t-il de nombres premiers inférieurs ou égaux à x ?

Lorsqu'on étudie la liste des nombres premiers, on constate rapidement qu'ils semblent de plus en plus rares, ce qui ne facilite pas leur recherche, comme vous pourrez le constater un peu plus loin. En fait, ils semblent répartis de façon tout à fait anarchique, sans règle.

Question 5 :

La répartition des nombres premiers a intrigué bien sûr les mathématiciens. Le nombre de nombres premiers inférieurs ou égaux à x est traditionnellement noté $\pi(x)$ (qui n'a rien à voir avec le nombre π). Dès 1798, Gauss avait émis l'hypothèse que $\pi(x)$ est, pour les grandes valeurs de x, approximativement égal à $\frac{x}{\ln x}$.

Vous trouverez en annexe la liste des 1000 premiers nombres premiers .

En utilisant cette liste, donnez-vous quelques valeurs assez grandes pour x, et comparez le nombre de nombres premiers inférieurs ou égaux à x, et le rapport $\frac{x}{\ln x}$.

Il peut sembler très étrange a priori que les logarithmes interviennent dans les nombres entiers. Pourtant, au 19° siècle, plusieurs mathématiciens essayèrent de démontrer la conjecture de Gauss. Ce sont finalement les mathématiciens Hadamard et de La Vallée Poussin, qui, en 1896, de façon indépendante, démontrèrent ce résultat : quand x tend vers l'infini, le rapport $\frac{\pi(x)}{\frac{x}{\ln x}}$ tend vers 1.

Ce théorème s'appelle **le théorème des nombres premiers**.

Pouvez vous, à l'aide de ce théorème, imaginer le nombre de nombres premiers inférieurs ou égaux à 10 000 000 ?

Construire des nombres premiers

Les mathématiciens s'efforcent depuis très longtemps de trouver des formules qui permettent de construire des nombres premiers.

* Fermat, au 17° siècle, a pensé que les nombres de la forme $2^{2^n}+1$ étaient premiers quel que soit n.

Question 6 : examiner les nombres de Fermat jusqu'à n = 5. Fermat avait-il raison ?

* Mersenne, au 17° siècle aussi, a étudié les nombres de la forme 2^p-1.

Question 7 : en utilisant la liste des nombres premiers fournie, trouver un nombre de Mersenne premier. Trouver aussi un nombre de Mersenne non premier.

On peut démontrer que si 2^p-1 est premier, alors p est premier ; mais la réciproque n'est pas vraie. Si p est premier, alors 2^p-1 ne l'est pas forcément.

Question 8 : trouver plusieurs nombres de la forme 2^p-1 avec p premier, qui ne sont pas premiers.

* On ne sait pas s'il existe une infinité de nombres de Mersenne premiers.

Des nombres un peu particuliers :

Les nombres premiers jumeaux : on appelle nombres premiers jumeaux deux nombres premiers dont la différence est 2. Ils peuvent donc être désignés par a et a + 2.Par exemple, 5 et 7 sont des nombres premiers jumeaux, ainsi que 857 et 859.

Question 9 : trouvez d'autres couples de nombres premiers jumeaux.

L'étude de ces nombres premiers jumeaux a fait naître une conjecture : il existe une infinité de nombre premiers jumeaux. Cette conjecture n'est toujours pas démontrée.

Les nombres parfaits : un nombre entier n est parfait si la somme de ses diviseurs propres (c'est à dire les diviseurs différents de n lui-même) est égale à n. 496 est un nombre parfait.

Question 10 : a) justifiez que 496 est un nombre parfait.

b) trouvez au moins un autre nombre parfait (inférieur à 496).

Dans les Éléments d'Euclide livre IX on trouve la proposition suivante :

> Proposition 36:
>
> Si autant de nombres qu'on voudra sont successivement exposés à partir de l'unité en raison double jusqu'à ce que leur tout devienne premier, et si ce tout multiplié par le dernier produit un nombre, le produit sera parfait.

Etre en raison double signifie être multiplié toujours par 2.

Ainsi la proposition 36 peut s'écrire :

Si $1+2+2^2+2^3+...+2^p$ est premier, alors $2^p(1+2+2^2+2^3+...+2^p)$ est parfait.

Question 11 : a) en utilisant les résultats sur les suites géométriques, écrire de façon plus simple $1+2+2^2+2^3+...+2^p$.

b) démontrez alors le résultat énoncé par Euclide.

Euler a démontré que tous les nombres parfaits pairs sont euclidiens, c'est à dire de la forme présentée par Euclide dans la proposition 36. On ne sait pas s'il existe des nombres parfaits impairs.

Au terme de cette petite exploration, nous pouvons retenir que l'infinitude des nombres premiers est de plus en plus mystérieuse. Avant de poursuivre le voyage, énonçons encore une conjecture non démontrée, la conjecture de Goldbach :

Dans une lettre à Euler en 1742, Goldbach émit l'hypothèse que tout entier est la somme de trois nombres premiers au plus. Vous pouvez constater la validité de cette idée sur quelques nombres. Cependant la conjecture de Goldbach n'est pas encore démontrée.

II. Tests de primalité

Etant donné un entier naturel N, ou bien il est premier, ou bien on peut le décomposer en un produit de facteurs premiers, on dit alors qu'il est composé. La connaissance de nombres premiers est donc un enjeu important en arithmétique, notamment en cryptographie où l'on utilise de grands nombres premiers.

Il existe un algorithme simple pour savoir si un nombre N est premier : il suffit de diviser N successivement par tous les entiers premiers p tels que $p \leq \sqrt{N}$; si aucun d'eux ne divise N, alors N est premier.

Ainsi, par exemple, 1607 est premier car 1607 n'est divisible par aucun des nombres premiers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 et 41. On s'arrête à 41 car $41^2 = 1681$ qui est supérieur à 1607.

Mais si N est un grand nombre, avec plusieurs dizaines de chiffres, la méthode devient inopérante car elle nécessite des heures, voire des années de calculs.

La mise au point de tests de primalité, c'est-à-dire de tests permettant de savoir si un nombre est premier, efficaces et rapides est donc depuis longtemps l'objet de recherches de la part des mathématiciens. Cette recherche va d'ailleurs de pair avec la recherche du « plus grand nombre premier »[1].

Nous allons présenter ici trois tests mais il en existe bien d'autres[2]. Les tests présentés ont été choisis pour leur (relative !) simplicité et parce qu'ils montrent comment les mathématiciens avancent dans la résolution des problèmes : les mathématiques ne se sont pas faites en un jour...

[1] L'ensemble des nombres premiers étant infini, il n'existe pas de plus grand nombre premier ; mais on cherche un nombre premier plus grand que le plus grand précédemment connu. Voir dans l'Annexe I « Les records ».
[2] Voir en Annexe 2 une courte présentation des tests probabilistes ; par ailleurs nous encourageons vivement le lecteur intéressé à lire « Histoire d'algorithmes » (édition Belin).

1. La réciproque du théorème de Fermat

Pierre de Fermat s'intéresse à la théorie des nombres après avoir lu l'*Arithmétique* de Diophante publiée en 1621 par Bachet de Méziriac. Il échange à ce sujet une correspondance notamment avec le Père Mersenne. En octobre 1640 il lui adresse une lettre dans laquelle il énonce ce que nous appelons actuellement « le petit théorème de Fermat »[3]. Il est à noter que Fermat n'a jamais donné la preuve de ce théorème ; c'est Euler qui en donnera une démonstration en 1736.

La lettre de Fermat

« Tout nombre premier mesure infailliblement une des puissances –1 de quelque progression que ce soit, et l'exposant de ladite puissance est sous multiple du nombre premier donné –1. Et après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont de même à la question.

Exemple, soit la progression donnée,

1	2	3	4	5	6	
3	9	27	81	243	729	etc...

avec ses exposants au dessus.

Prenez, par exemple, le nombre 13, il mesure la troisième puissance –1, de laquelle 3 exposant est sous multiple de 12 qui est moindre de l'unité que le nombre de 13. Et parce que l'exposant de 729 qui est 6 est multiple du premier exposant 3 il s'ensuit que 13 mesure aussi ladite puissance de 729-1. Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers. De quoi je vous enverrais la démonstration, si je n'appréhendais d'être trop long ».

[3] Cette appellation est donnée par opposition au « grand théorème de Fermat » dont l'énoncé est : lorsque n est un entier supérieur ou égal à 3, l'équation $x^n + y^n = z^n$ n'a pas de solution en nombres entiers, hormis la solution x=y=z=0. La démonstration de ce théorème a finalement été trouvée par Andrew Wiles en octobre 1994. On pourra lire à ce sujet le passionnant livre de Simon Singh « Le dernier théorème de Fermat » (édition Hachette Littératures, collection Pluriel).

L'énoncé actuel de ce théorème est le suivant :

Soient a et p deux entiers premiers entre eux. Si p **est premier** alors p **divise** $a^{p-1}-1$.

- *Question : La version moderne du théorème est-elle la traduction littérale du texte de Fermat ?*

Ce théorème permet d'affirmer qu'un entier p est composé :

En effet prenons $a = 3$ et $p = 341$, a et p sont premiers entre eux.. 341 **ne divise pas** $3^{340}-1$ donc 341 **n'est pas premier**.

Mais ce théorème ne permet pas d'affirmer qu'un nombre p est premier : la réciproque est fausse.

En voici un contre-exemple :

Prenons $a = 2$ et $p = 341$, a et p sont premiers entre eux ; 341 divise $2^{340}-1$ et pourtant 341 n'est pas premier (341 = 11 x 31).

Exercice : 1°) Vérifier que 3 et 341 d'une part, 2 et 341 d'autre part sont premiers entre eux.

2°) Déterminer le reste de la division par 341 de 3^{10}, de 56^3.
En déduire le reste de la division par 341 de 3^{340} puis de $3^{340}-1$. Conclure.

3°) De même, déterminer le reste de la division par 341 de 2^{10}.
En déduire le reste de la division par 341 de $2^{340}-1$.Conclure.

Fermat

Le mathématicien Lucas (1842-1891), en 1876, rajoute une hypothèse supplémentaire qui permet d'établir la « réciproque » du théorème de Fermat.

Le texte de Lucas

Si $a^x - 1$ est divisible par n, pour x égal à $(n-1)$, et n'est pas divisible par n pour x égal à une partie aliquote[4] de $(n-1)$, le nombre n est premier.

Nous avons énoncé pour la première fois ce théorème en 1876, au Congrès de l'Association française pour l'Avancement des Sciences, à Clermont-Ferrand, dans une note intitulée : *Sur la recherche des grands nombres premiers.* Nous en donnerons, dans le second volume, un grand nombre de corollaires.

Exemple I. Soit $a = 3$, $n = 65537 = 2^{16}+1$;

Les diviseurs de $(n-1)$ sont $1, 2, 2^2, 2^3, 2^4, 2^5, \ldots, 2^{16}$.

Si on calcule les restes par n des puissances de 3 dont les exposants sont égaux aux termes de la suite précédente, en observant que chaque reste s'obtient en divisant par n le carré du reste précédent, on trouve[5] 3, 9, 81, 6561, -11088, ..., -1, et, puisqu'il n'y a aucun reste égal à 1 avant le dernier de la suite, on en conclut que $2^{16}+1 = 65537$ est un nombre premier.

Extrait de la *Théorie des nombres* (1891), réédition Blanchard, Paris, 1961

La machine arithmétique de Pascal

[4] Une partie aliquote d'un nombre est un diviseur de ce nombre autre que lui-même.

[5] Dans la définition de la division euclidienne utilisée au lycée, le reste est un entier naturel ; la suite des restes est alors 3, 9, 81, 6561, 54449, 61869, ..., 65536.

Ce test de primalité a plusieurs défauts relevés par le mathématicien américain Lehmer (1905-1991) dans un article paru en 1927 :

Le texte de Lehmer

Théorème 1. Si $a^x \equiv 1 \pmod N$ pour $x = N-1$, mais non pour x diviseur propre de $N-1$, alors N est premier.

Quand on l'applique à un N particulier, ce théorème présente trois défauts. Premièrement, la factorisation complète de $N-1$ doit être connue. Deuxièmement, le nombre de valeurs de x qui doivent être essayées de façon à montrer que la seconde condition de l'hypothèse est remplie, peut être très grande. Troisièmement, la condition de primalité est suffisante mais pas nécessaire. Si, toutefois, N est de la forme 2^n+1, les deux premiers défauts s'évanouissent ; car dans ce cas tous les diviseurs de $N-1$ sont des puissances de 2, aussi en testant la première partie de l'hypothèse, la seconde partie est automatiquement vérifiée par le calcul des carrés successifs des restes modulo N. Malheureusement les seuls nombres de la forme 2^n+1 qui ont une chance d'être premiers sont les nombres de Fermat pour lesquels n est une puissance de 2. Les nombres $2^{128}+1$ et $2^{256}+1$ ont été testés par Morehead et A.E.Western, et ces deux nombres ont été trouvés composés. Le nombre de Fermat suivant est $2^{1024}+1$, un nombre de 309 chiffres. Un calculateur habile pourra tester ce nombre en une dizaine d'années. Autant que le sache le présent auteur, aucun nombre premier hors de portée des méthodes de factorisation ordinaires n'a jamais été identifié par la réciproque du théorème de Fermat. Il est clair que le théorème doit être amélioré avant que davantage de résultats soient possibles.[...]

L'amélioration suivante du théorème 1 qui se suggère d'elle-même est la réduction du nombre de valeurs de x à essayer.

Dans le théorème suivant ce nombre est réduit du nombre de diviseurs de $N-1$ au nombre de ses facteurs premiers.

Théorème 2. Si $a^x \equiv 1 \pmod N$ pour $x = N-1$, mais non pour x quotient de $N-1$ par division d'un de ses facteurs premiers, alors N est premier.

[...]

Théorème 3. Si $a^x \equiv 1 \pmod N$ pour $x = N-1$ et si $a^x \equiv r > 1 \pmod N$ pour $x = (N-1)/p$, et si $r-1$ est premier avec N, alors tous les facteurs premiers de N sont de la forme $np^\alpha + 1$ où α est la plus grande puissance du nombre premier p qui divise $N-1$.

[...]

Extrait de *Tests for primality by the converse of Fermat's theorem*, Bulletin of the American Mathematical society, vol.33 (1927). Reproduit dans *Selected papers of D.H.Lehmer*, ed. Mc Carthy, The Charles Babbage Research Centre, vol.1, Winnipeg, 1981, pp. 70-79. Trad. E.Barbin.

Lehmer fait fonctionner l'algorithme déduit du théorème 3 sur le nombre $N = 9\,999\,999\,900\,000\,001$ qui est le quotient $\frac{10^{24}+1}{10^{8}+1}$ et démontre que N est premier. Si Lehmer a choisi ce nombre ce n'est pas par hasard ! En effet son algorithme est assez performant lorsque $N-1$ a peu de facteurs premiers, ce qui est le cas ici ($N-1 = 2^8 \times 5^8 \times 3^2 \times 11 \times 73 \times 101 \times 137$). Avant l'invention des ordinateurs il fallait bien choisir ses exemples et faire preuve d'habileté dans les calculs !

2. Le test de Lucas :

Lucas, à la suite de nombreux mathématiciens tels que Lagrange, Legendre, Gauss, s'intéresse aux propriétés arithmétiques des suites récurrentes (suites de Fibonacci et autres suites voisines). Cela le conduit à construire un test de primalité efficace bien adapté aux nombres de la forme $2^m - 1$ (nombres de Mersenne). Grâce à ce test Lucas établit en 1876 que $2^{127} - 1$ est premier, nombre qui restera, jusqu'en 1952 (?), le plus grand nombre premier connu. Avec l'invention des ordinateurs le test de Lucas a permis d'en découvrir de nouveaux, par exemple le nombre $2^{110503} - 1$ découvert en 1988.

Le test n'est toutefois pas d'une compréhension très aisée aussi nous contenterons-nous de laisser Lucas en vanter les mérites :

> « Cette méthode de vérification des grands nombres premiers, qui repose sur le principe que nous venons de démontrer, est la *seule méthode directe et pratique*, connue actuellement, pour résoudre le problème en question.[...] Pour vérifier la dernière assertion du Père Mersenne, sur le nombre supposé premier $2^{257} - 1$, et qui a soixante-dix-huit chiffres, il faudrait à l'humanité toute entière, formée de mille millions d'individus, calculant simultanément et sans interruption, un temps supérieur à un nombre de siècles représenté par un nombre de vingt chiffres ; par notre méthode il suffit d'effectuer successivement les carrés de 250 nombres ayant 78 chiffres, au plus ; cette opération ne demanderait pas, à deux calculateurs habiles contrôlant leurs opérations, plus de huit mois de travail. »

3. Le test de Pépin (1826-1904)

Il s'agit d'un algorithme efficace pour tester la primalité des nombres de Fermat, c'est-à-dire des nombres de la forme $F_n = 2^{2^n} + 1$ .Fermat affirmait que tous les nombres de cette forme étaient premiers, et qu'il l'avait d'ailleurs démontré. En 1732 Euler prouve que cette conjecture est fausse en établissant que $F_5 = 2^{32} + 1$ est composé ($F_5 = 641 \times 6700417$). Depuis, la recherche des nombres de Fermat premiers ne s'est jamais interrompue.

A la fin du XIXème siècle on s'interroge sur la primalité de F_6. Lucas prétend qu'avec son test il suffit de 30 heures de calculs pour le savoir. Pépin, lui, dans l'article où il présente son test donne la liste des 63 congruences à calculer pour conclure si F_6 est premier ou pas.

Le test de Pépin a permis, avec l'apparition des ordinateurs, de tester de grands nombres de Fermat. Le plus grand nombre de Fermat exploré avec le test de Pépin est F_{14} : ce nombre est formé de 315653 chiffres, il est composé mais on ne connaît, à l'heure actuelle, aucun de ses facteurs !

Enoncé du test de Pépin

Théorème : La condition nécessaire et suffisante pour que le nombre $a_n = 2^{2^n} + 1$ soit premier, quand n>1, est que le nombre $5^{(a_n-1)/2} + 1$ soit divisible par a_n.

(suit la démonstration au cours de laquelle Pépin note (2) la congruence $5^{(a_n-1)/2} + 1 \equiv 0 \pmod{a_n}$ *et il termine ainsi :)*

Pour reconnaître si la congruence (2) est vérifiée, oui ou non, on formera la suite (A) $5^2, 5^4, 5^8, \cdots, 5^{(a_n-1)/2}$, composée de $2^n - 1$ termes, dont chacun est le carré du précédent ; mais on aura soin de réduire chaque terme à son résidu minimum suivant le module a_n, de sorte que toutes les opérations nécessaires se réduiront à élever au carré des termes dont le nombre des chiffres ne surpasse jamais celui des chiffres de a_n. Soit, par exemple, n = 6 ; la suite (A) se compose de soixante-trois termes, le nombre a_6 est premier ou composé suivant que le résidu positif minimum du soixante-troisième terme se réduit, oui ou non, au nombre $a_n - 1 = 2^{64}$.

Au lieu de tester la primalité des nombres, une autre voie explorée par les mathématiciens a été d'essayer de trouver une formule permettant de fabriquer des nombres premiers. Euler a proposé la formule $n^2 - n + 41$ qui fournit un nombre premier pour n allant de 1 à 40 mais pas pour n = 41. Des mathématiciens ont trouvé en 1976 un polynôme de degré 25 avec 26 variables tel que l'ensemble des nombres premiers est exactement l'ensemble des valeurs positives prises par ce polynôme quand on remplace ses variables par des entiers naturels.

Mersenne

Diophante, traduit par Bachet de Méziriac

Exemplaire de Fermat

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT *Senatoris Tolosani.*

Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiuſdem D. de FERMAT Epiſtolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX. M

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis unitatibus 10. aequatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quaestioni.

[illegible]

IN QVAESTIONEM VII.

Conditionis appositae eadem ratio est quae & appositae praecedenti quaestioni, nil enim aliud requirit quam ut quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVAESTIO VIII.

Propositum quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. aequales esse quadrato. Fingo quadratum a numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto a 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. haec aequabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & a similibus auferantur similia, fient 5 Q. aequales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter vero $\frac{144}{25}$. & vtriusque summa est $\frac{400}{25}$. seu 16. & vterque quadratus est.

[illegible]

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVAESTIO IX.

Rursus oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius vero quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille vero 4 Q. + 16. − 16 N. Caeterum volo vtrumque simul aequari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. aequatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

[illegible]

3 - Autour des "Recherches arithmétiques" de Gauss

I Des nombres congrus :

En 1801, **Karl-Friedrich Gauss**, qui n'a que 24 ans, publie un ouvrage magistral, qui marquera le début de la théorie moderne des nombres. Il s'agit de "**Disquisitiones arithmeticae**", (**Recherches arithmétiques**). Il y reprend et synthétise les questions d'arithmétique examinées par ses illustres prédécesseurs ou contemporains, tels Fermat, Euler, Lagrange. Il précise de nombreuses démonstrations, il explore de façon rigoureuse et mène à leur aboutissement de nombreux résultats qui avaient pu être énoncés avant lui, en particulier ce que l'on appelle la loi de réciprocité quadratique. Nous ne nous attacherons pas à cette partie de l'ouvrage de Gauss, mais plutôt aux deux premières parties, plus élémentaires, mais fondatrices de l'arithmétique.
Les Recherches arithmétiques comportent en effet sept sections :

Nombres congruents en général
Congruences du premier degré
Résidus de puissance
Congruences du second degré
Formes et équations indéterminées du second degré
Diverses applications des questions étudiées précédemment
Equations définissant les sections d'un cercle.

Gauss est en effet l'inventeur de la notion de congruence et de la notation toujours utilisée "≡".
Nous vous proposons les deux premières pages de la section première, car il est difficile de présenter de façon plus simple et plus explicite ce que l'on entend par "**nombres congrus**".

RECHERCHES ARITHMÉTIQUES.

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

A

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*

(*) 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.

Les propriétés des congruences facilitent grandement la recherche de problèmes de divisibilité entre autres.
Voici quelques exercices pour juger de la simplification que la notion de congruence peut offrir :

Exercice 1 :
Trouver le reste de la division de 3^{1604} par 34.

Exercice 2 :
Montrer que $2^{70} + 3^{70}$ est divisible par 13.

Exercice 3 :

Dans le chapitre 2, vous avez dû constater que le nombre de Fermat $F_5 = 2^{2^5} + 1$ n'est pas premier ; il est divisible par 641. Nous vous proposons de le démontrer en utilisant les congruences.
1° Montrer que : $5^4 \equiv -2^4 \pmod{641}$. Et que $5 \times 2^4 \equiv -1 \pmod{641}$.
2° En déduire que $2^{32} + 1$ est divisible par 641.

Munis maintenant de l'outil des congruences, nous pouvons continuer cette exploration de quelques résultats démontrés par Gauss.
Pour aller plus loin vous trouverez en annexe 3 un texte de **Pascal** sur les critères de divisibilité des nombres, que nous vous proposons de retranscrire en termes de congruences.

II Le théorème de Gauss, théorème clef de l'arithmétique ?

Dans un manuel contemporain, le plus souvent, nous trouverons :
Une démonstration du "**théorème de Bézout**", puis de "**l'identité de Bézout**", à l'aide de l'algorithme d'Euclide, puis, comme conséquence directe, le "**théorème de Gauss**", ce théorème de Gauss, permettant de démontrer l'unicité de la décomposition en produit de facteurs premiers.
Le théorème de Gauss est en général énoncé sous la forme :

Si un nombre a divise le produit bc, et si a et b sont premiers entre eux, alors a divise c.

(Les nombres considérés sont bien sûr des nombres entiers).

Ce théorème est parfois appelé théorème de Bézout-Gauss, car sa démonstration s'appuie sur le **théorème de Bézout**.

Vous trouverez en général ce théorème dit de Bézout sous cette forme :

a et b étant deux entiers, il existe un couple (u , v) d'entiers relatifs tels que :

au + bv = pgcd (a , b).

Il sera distingué de l'identité de Bézout (ce qui est utilisé pour la démonstration du théorème de Gauss), qui peut s'énoncer sous la forme :

a et b étant deux entiers, les phrases suivantes sont équivalentes :

f) il existe un couple (u,v) d'entiers relatifs tels que au + bv = 1

g) a et b sont premiers entre eux.

En fait l'identité dite de **Bézout** [9] devrait porter le nom de **Bachet**,[10] car sa démonstration se trouve dans la deuxième édition de ses **Problèmes plaisants et délectables** en 1624. Il y énonce en effet le problème suivant :

Deux nombres premiers entre eux étant donnés, trouver le moindre multiple de chacun d'iceux, surpassant de l'unité un multiple de l'autre.

Ce que nous énoncerions sous la forme :

a et b étant deux entiers premiers entre eux donnés, trouver x et y entiers relatifs tels que :

$$ax = by + 1.$$

Il donne une solution générale du problème en utilisant l'algorithme d'Euclide.

Néanmoins, voici ce que vous trouverez dans le cours de Bézout de 1764-1767:

---

[9] Etienne Bézout (1730-1783), professeur de mathématiques auprès des gardes de la marine, puis examinateur pour l'artillerie, est surtout connu pour ses ouvrages pédagogiques, en particulier son **Cours complet de mathématiques à l'usage de la Marine et de l'artillerie**, en six volumes, qui connut un grand nombre de rééditions. La première parution date de 1780. Il avait déjà publié un cours de mathématiques en 1764-1765, où nous trouvons le texte proposé. Bézout fit aussi un travail important sur la résolution des équations algébriques, généralisant des travaux de Cramer sur les déterminants. Ces travaux furent publiés dans Théorie générale des équations algébriques en 1779. Il fut élu à l'Académie de sciences en 1758.

[10] Claude Gaspard Bachet de Méziriac (1581-1638) était passionné de langues anciennes et à la fois mathématicien, poète, philosophe ... Il est particulièrement célèbre pour sa traduction en latin de l'**Arithmétique** de Diophante (1621), puisque c'est en marge de son exemplaire que Fermat écrivit son dernier fameux théorème. Il est aussi connu pour ses **Problèmes plaisants et délectables qui se font par les nombres** (1613), qui nous occupent ici. Il entra à l'AcadémieFfrançaise qui venait d'être créée en 1635.

Le texte de Bézout

Extrait du *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine*, 6 vol., 1764-1769. Troisième Partie contenant l'Algèbre et l'Application de cette Science à l'Arithmétique et la Géométrie, Musier, Paris, 1766 (fac-similé des pp. 118-121).

Des Problèmes indéterminés

Queſtion premiere. *On demande en combien de manieres on peut payer 542 livres, en donnant des pieces de 17 liv. & recevant en échange des pieces de 11 livres.*

Repréſentons par x le nombre des pieces de 17 liv. & par y celui des pieces de 11 liv.; en donnant x pieces de 17 liv. on payera x fois 17 liv. ou $17x$: en recevant y pieces de 11 liv. on recevra $11y$; par conſéquent, on aura payé $17x - 11y$; & puiſqu'on veut payer 542 liv. on aura $17x - 11y = 542$. Tirons la valeur de y, c'eſt-à-dire, de l'inconnue qui a le moindre coëfficient, & nous aurons $y = \frac{17x-542}{11}$.

Comme on n'a que cette équation, on voit qu'en mettant arbitrairement pour x tel nombre qu'on voudra, on aura pour y une valeur qui ſatisfera ſûrement à l'équation; mais comme la queſtion exige que x & y ſoient des nombres entiers, voici comment il faut s'y prendre pour y parvenir directement.

La valeur de $y = \frac{17x-542}{11}$ ſe réduit, en faiſant la diviſion autant qu'il eſt poſſible, à $y = x - 49 + \frac{6x-3}{11}$; il faut donc que $\frac{6x-3}{11}$ ſoit un nombre entier: ſoit u ce nombre entier; on aura $\frac{6x-3}{11} = u$, & par conſé-

.../...

quent $6x - 3 = 11u$ & $x = \frac{11u+3}{6}$, ou, en faiſant la diviſion, $x = u + \frac{5u+3}{6}$; il faut donc que $\frac{5u+3}{6}$ faſſe un nombre entier : ſoit t ce nombre entier ; on aura $\frac{5u+3}{6} = t$, & par conſéquent $5u + 3 = 6t$ & $u = \frac{6t-3}{5} = t + \frac{t-3}{5}$; il faut donc que $\frac{t-3}{5}$ faſſe un nombre entier : ſoit s ce nombre entier, on aura $\frac{t-3}{5} = s$, & par conſéquent $t = 5s+3$: l'opération eſt terminée ici, parce qu'il eſt évident qu'en prenant pour s tel nombre entier qu'on voudra, on aura toujours pour t un nombre entier tel que l'exige la queſtion, puiſqu'il n'y a plus de dénominateur.

Remontons maintenant aux valeurs de x & y : puiſqu'on a trouvé $u = \frac{6t-3}{5}$; en mettant pour t ſa valeur $5s + 3$, on aura $u = \frac{30s+18-3}{5} = 6s + 3$: & puiſqu'on a trouvé $x = \frac{11u+3}{6}$, en mettant pour u ſa valeur, on aura $x = \frac{66s+33+3}{6} = 11s + 6$: enfin, puiſqu'on a trouvé $y = \frac{17x-542}{11}$, en ſubſtituant pour x ſa valeur, on aura $y = \frac{187s+101-142}{11} = 17s - 40$; ainſi les valeurs correſpondantes de x & de y ſont $x = 11s + 6$, & $y = 17s - 40$. Par la premiere, on eſt libre de prendre pour s tel nombre entier qu'on voudra ; mais la ſeconde ne permet pas de prendre s plus petit que 3 ; en effet y devant être poſitif, il faut que $17s$ ſoit plus grand que 40, ou que s ſoit plus grand que $\frac{40}{17}$, c'eſt-à dire, plus grand que 2.

On peut donc ſatisfaire à cette queſtion d'une infinité de manieres différentes, qu'on aura toutes en mettant dans les valeurs de x & de y, au lieu de s, tous les nombres entiers poſitifs imaginables depuis 3 juſqu'à l'infini ; ainſi poſant ſucceſſivement $s = 3$, $s = 4$, $s = 5$, $s = 6$, $s = 7$, &c, on aura les valeurs correſpondantes de x & de y comme il ſuit :

$x = 39 \ldots$	$y = 11$
$= 50$	$= 28$
$= 61$	$= 45$
$= 72$	$= 62$
$= 83$, &c.	$= 79$

Dont chacune eſt telle qu'en donnant le nombre de pieces de 17 liv. déſigné par x, & recevant le nombre correſpondant de pieces de 11 liv. déſigné par y, on payera 542 livres.

Exercice 1:

A la manière de Bézout, ou avec des procédés plus contemporains équivalents, résoudre le problème suivant :
Des astronomes ont pu observer deux planètes inconnues d'un certain observatoire situé en un lieu secret A. La première planète est passée à la verticale de A le 2 janvier 1999 ; la deuxième est passée à la verticale de A le 5 janvier 1999. D'après leurs observations, la première planète repasse tous les 567 jours à la verticale de A ; la deuxième repasse tous les 145 jours à la verticale de A; Combien de jours se seront écoulés à partir du 1° janvier 1999, jusqu'à ce que les deux planètes passent à la verticale de A le même jour ?

Exercice 2 : identité de Bézout et géométrie :

Soit a et b deux entiers premiers entre eux. Soit A le point de coordonnées (a ; b) dans un repère orthonormal $(O, \vec{i}, \vec{j})$ du plan.
Déterminer l'ensemble des points M de coordonnées entières (u , v) tels que au + bv = 1.
(On pourra traduire l'égalité précédente sous la forme d'un produit scalaire).

Exercice 3 :

Retrouver la démonstration du "théorème de Gauss" à l'aide de "l'identité de Bézout" tels qu'ils sont énoncés en début de ce chapitre.

Nous noterons que les noms donnés aux théorèmes cités sont d'origine assez récente ; ils ne doivent pas masquer que les découvertes en mathématiques sont rarement l'œuvre d'une seule personne. Ils vont cependant nous donner l'occasion de dénouer un peu les fils de l'histoire .
Nous pourrons peut-être alors nous demander pourquoi le "théorème de Gauss" a pu être considéré comme le théorème clef de l'arithmétique,. Si nous considérons en effet ce qui vient d'être étudié, cet adjectif semblerait plutôt s'appliquer au théorème ou à l'identité de Bézout.
C'est la décomposition d'un entier en produit de facteurs premiers qui sera peut-être la clef.

1 Les Éléments d'Euclide :

Les Éléments d'Euclide une fois de plus constitueront notre première étape. Jean Itard[11] note que ce qui sera appelé plus tard "théorème de Gauss" n'apparaît pas dans les éléments d'Euclide, mais qu'il se trouvera énoncé pour la première fois dans les "**Nouveaux éléments**" de **J. Prestet**, en 1689.
La proposition 31 du livre VII des éléments d'Euclide permet d'affirmer que tout entier peut se décomposer en produit de facteurs premiers :

Livre VII, proposition 31 :
Tout nombre composé admet un diviseur premier

Question 1:

Appelez a un nombre composé (c'est à dire non premier), et démontrez cette proposition.
Démontrez ensuite que tout entier est soit premier, soit décomposable en un produit de facteurs premiers.

2 Le théorème de Gauss et l'unicité de la décomposition en facteurs premiers :

Comme nous l'avons noté plus haut, la Section première des "**Recherches arithmétiques**" est consacrée à la définition de ce que Gauss appelle congruence, et aux résultats qui en découlent.
C'est dans la Section seconde, Des congruences du premier degré, que se trouvent les énoncés et démonstrations qui nous préoccupent ici.
Contrairement à ce que l'on pourrait penser, nous ne trouvons pas dans les "Recherches arithmétiques" l'enchaînement actuel traditionnel des résultats.
Les travaux de **Fermat** en théorie des nombres n'avaient pas été vraiment poursuivis par les mathématiciens, jusqu'au XVIII° siècle. **Euler** est un des premiers qui s'y intéressera[12], et il présente comme un procédé non usuel mais performant, la recherche du PGCD ou du PPCM de deux nombres à l'aide de la décomposition en produit de facteurs premiers. Cette méthode suppose, si les nombres sont un peu grands, d'être un brillant calculateur, contrairement à l'utilisation de l'algorithme d'Euclide. Elle suppose aussi d'avoir démontré l'unicité de la décomposition. Dès le début de la section seconde, Gauss signale que souvent, à tort, cette unicité est supposée implicitement. Il va ainsi la démontrer très rapidement.
Nous trouvons successivement dans la section seconde :

---

[11] Jean Itard, *Les livres arithmétiques d'Euclide*, Paris, 1961

[12] Par exemple dans son ouvrage "Essai d'une nouvelle théorie de la musique", en 1731. Voir Anne Boyé, *Sur l'essai d'une nouvelle théorie de la musique de L. Euler*, Sciences et techniques en perspective, vol. 23, Université de Nantes, Centre Viète.

13 : Théorème : le produit de deux nombres positifs plus petits qu'un nombre premier donné ne peut être divisé par ce nombre premier.

14 : Si aucun des nombres a et b n'est divisible par un nombre premier p, le produit ab ne le sera pas non plus.

Nous avons ici d'une manière non directe, un énoncé proche du "Théorème" dit "de Gauss". Gauss signale que ce résultat a été démontré par Euclide. Il le place ici cependant avec sa démonstration car celle-ci est exemplaire de la méthode qu'il va utiliser. Examinons donc sa méthode

Soient α et β les résidus minima positifs des nombres a et b, suivant le module p, aucun d'eux ne sera nul par hypothèse. Or si l'on avait $ab \equiv 0$, comme $ab \equiv \alpha\beta$, on aurait $\alpha\beta \equiv 0$, ce qui serait contraire au théorème précédent.

Question 2 : *(Pour aider à comprendre cette démonstration)*

Que signifie à votre avis l'expression : résidus minima positifs ?

Par exemple quel est le résidu minimum positif de 13 suivant le module 3, puis celui de 11 suivant le module 7 ?

Essayer de rédiger de façon plus contemporaine la démonstration de Gauss.

Quel sorte de raisonnement utilise-t-il ?

Ce dernier résultat permet à Gauss d'énoncer et de démontrer le théorème 16 qui semble majeur à ses yeux.

Théorème 16 : un nombre composé ne peut se résoudre que d'une seule manière en facteurs premiers.

La démonstration de ce théorème a déjà été donnée par Euclide, *El.* VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parce que plusieurs auteurs modernes ont présenté des raisonnemens vagues au lieu de démonstration, ou bien ont négligé ce théorème; que dans le but de faire mieux saisir, par ce cas très-simple, l'esprit de la méthode que nous appliquerons par la suite à des points bien difficiles.

15. *Si aucun des nombres* a, b, c, d, *etc. n'est divisible par le nombre premier* p, *le produit* abcd, *etc. ne le sera pas non plus.*

Suivant l'article précédent, *ab* n'est pas divisible par *p*; donc il en est de même de *abc*, et ainsi de suite.

16. THÉORÈME. *Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.*

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

17. Si donc le nombre *A* est le produit de *B*, *C*, *D*, etc., il s'ensuit que les nombres *B*, *C*, *D*, etc ne peuvent avoir de facteurs premiers différens de ceux de *A*, et que chacun de ces facteurs doit

Pour aider à comprendre cette démonstration :

La démonstration de Gauss comporte deux étapes qui s'appuient toutes les deux sur les résultats 14 et 15 :
Supposant qu'un nombre A se décompose en facteurs premiers de deux façons différentes, il est démontré
1° que les facteurs premiers de chaque décomposition sont les mêmes ;
2° que chaque facteur premier apparaît avec la même puissance dans les deux décompositions.

Pour entrer plus dans le détail :

Supposons que A = $a^{\alpha}b^{\beta}c^{\gamma}...p^{m}...$, où a, b, c sont des nombres premiers distincts, et qu'il existe une autre décomposition de A en produit de facteurs premiers.
1° Justifier que cette autre décomposition ne pourrait contenir que les facteurs premiers a, b, c, ...,p .. et tous ceux là.
Ainsi : A = $a^{\alpha}b^{\beta}c^{\gamma}...p^{m}... = a^{\alpha'}b^{\beta'}c^{\gamma'}...p^{m'}..$
2° Si p est un facteur de A, avec la puissance m dans la première décomposition et m' dans la deuxième, avec m < m', divisant de part et d'autre par p^m, le facteur p n'apparaît plus dans la première décomposition, mais il subsiste dans la deuxième. Conclure que c'est impossible (en utilisant le même raisonnement qu'au 1°).

Ce théorème sert immédiatement à déterminer le PPCM et le PGCD de 2 ou plusieurs nombres.

Exercice :
1° A l'aide de la décomposition en produit de facteurs premiers, déterminer le PGCD et le PPCM des entiers : 304, 2880 et 864.
2° Dans le chapitre sur l'algorithme d'Euclide, vous avez déterminé le PGCD de 1 100 005 423 et de 1 100 000 077. L'utilisation de la décomposition en produit de facteurs premiers vous semblerait-elle ici pertinente ?

Le "théorème de Gauss" :

L'énoncé actuel du théorème de Gauss se trouve immédiatement après, au point 19, mais très incidemment, caché au milieu d'autres résultats. L'énoncé 14 du début de la section seconde était en

fait suffisant. Nous remarquerons cependant qu'il n'est pas démontré à l'aide du théorème dit de Bézout.

19. *Si les nombres* a, b, c, etc. *sont premiers avec* k, *leur produit l'est aussi.*

En effet, puisqu'aucun des nombres a, b, c, etc. n'a de facteurs premiers communs avec k, et que le produit de ces nombres ne peut avoir de facteurs premiers qui n'appartiennent à quelqu'un d'entr'eux, ce produit n'aura non plus aucun facteur premier commun avec k.

Si les nombres a, b, c, *etc. sont premiers entr'eux, et que* k *soit divisible par chacun d'eux, il le sera aussi par leur produit.*

C'est une suite des nos 17 et 18. Soit en effet p un diviseur premier quelconque du produit abc etc. et qu'il ait l'exposant π, quelqu'un des nombres a, b, c, etc. sera divisible par p^π, parconséquent k. qui est divisible par ce nombre, le sera aussi par p^π : il en sera de même des autres diviseurs du produit.

Donc, *si deux nombres* m, n *sont congrus suivant plusieurs modules* a, b, c, etc. *premiers entr'eux, ils le seront aussi suivant leur produit.* En effet, puisque $m - n$ est divisible par chacun des nombres a, b, c, etc., il le sera aussi par leur produit.

Enfin, *si* a *est premier avec* b, *et que* ak *soit divisible par* b, k *sera aussi divisible par* b. En effet, puisque ak est divisible par a et par b, il le sera par leur produit ; donc $\frac{ak}{ab} = \frac{k}{b}$ sera un entier.

Question : repérez-vous l'énoncé actuel du "**Théorème de Gauss**" ?

En conclusion de cette partie, il semble justifié de dire que, dans la construction des "Recherches arithmétiques" du moins, ce que nous dénommons le théorème de Gauss, est bien le théorème clef de l'arithmétique, que ce soit dans la version indirecte, ou dans la version plus classique.

3 L'identité de Bézout :

Au point 25, Gauss va éclairer le titre de la section seconde : Des congruences du premier degré.

25 Nous appellerons *congruence* l'expression de deux quantités congrues, à l'instar des équations ; si elle renferme une inconnue, la *résoudre* c'est trouver pour l'inconnue une valeur qui satisfasse à la congruence. (...)
Quant aux congruences algébriques, elles se divisent selon la plus haute puissance de l'inconnue, en congruences du premier degré, du second degré, etc... On peut même proposer plusieurs congruences qui renferment plusieurs inconnues, et de l'élimination desquelles nous traiterons.

Gauss propose alors au point 27 de s'intéresser aux congruences où il s'agit de déterminer x et y entiers pour que ax = by ±1, a et b étant deux entiers donnés. Le procédé qu'il conseille est l'utilisation classique de l'algorithme d'Euclide. Il ne développe pas outre mesure ce point, car la solution, dit-il, est connue. Nous reconnaissons l'identité de Bézout, que nous avons étudiée un peu plus haut.

Question :
Pourquoi Gauss présente-t-il l'identité de Bézout sous cette forme ? En particulier, pourquoi ce ± 1 ?

Il est remarquable que celle-ci vient en bout de course dans cette section seconde, et n'a pas été utilisée pour démontrer les résultats précédents, contrairement à notre tradition actuelle.
Gauss ici, présente cependant un aspect inhabituel de résolution, dérivé de l'algorithme d'Euclide, mais classiquement moins usité : l'utilisation des fractions continues.

28 Lagrange[13] a traité le problème d'une manière un peu différente. Il observe que si l'on réduit la fraction $\frac{a}{b}$ en fraction continue :

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + etc... \quad + \cfrac{1}{\mu + \cfrac{1}{n}}}}}$$

et qu'après avoir effacé sa dernière partie $\frac{1}{n}$, on la ramène à une fraction ordinaire $\frac{x}{y}$, on aura $ax = by \pm 1$. Au reste les deux méthodes conduisent au même algorithme. Les recherches de Lagrange se trouvent dans *l'Histoire de l'Académie de Berlin*, année 1767, avec d'autres, dans les *Additions à l'Algèbre d'Euler*.

Exercice 5 :

Prenez les nombres a = 43 et b = 35. Il s'agit de trouver x et y entiers, pour que 43x + 35 y = 1.

$43 = 1 \cdot 35 + 8$ donc $\frac{43}{35} = 1 + \frac{8}{35}$

$35 = 4 \cdot 8 + 3$ donc $\frac{35}{8} = 4 + \frac{3}{8}$ et $\frac{43}{35} = 1 + \frac{1}{4 + \frac{3}{8}}$

$8 = 2 \cdot 3 + 2$ donc $\frac{8}{3} = 2 + \frac{2}{3}$ et $\frac{43}{35} = 1 + \frac{1}{4 + \frac{1}{2 + \frac{2}{3}}}$

Continuer l'algorithme d'Euclide, pour obtenir le développement en fractions continues, et conclure.

Voici d'autres petits exercices pour vous entraîner à utiliser les résultats énoncés par Gauss :

Exercice 6 : Problème des cent volailles

Ce problème a été posé par Zhang Qiujiang, mathématicien chinois, vers l'an 475 ; son auteur ne se doutait sans doute pas qu'il aurait un succès mondial. En effet, on le retrouve sous une forme différente en Inde au VIIème siècle, puis il apparaît simultanément en Egypte et en Europe du Nord au IXème siècle, ce qui constitue une diffusion d'une rapidité remarquable.

Un coq vaut cinq deniers de bronze ; une poule vaut trois deniers de bronze ; trois petits poussins valent un denier de bronze. Un homme achète cent volailles pour cent deniers. Combien de coqs, de poules et de poussins a-t-il achetés ?

---

[13] Joseph Louis Lagrange (1736 -1813), né à Turin ; prendra contact avec les travaux de Newton, Leibniz, Euler et des Bernoulli, par l'étude de l'Instituzione de Maria Gaetana Agnesi. Il travaillera particulièrement sur la résolution des équations algébriques, et la théorie des fonctions. On lui doit entre autre la notation f '(x), f "(x), ... pour les dérivées.

1°) En posant x, y, z les nombres respectifs de coqs, poules et poussins achetés, établir que le problème a pour solutions les solutions du système

$\begin{cases} z = 100 - (x + y) \\ 7x + 4y = 100 \end{cases}$ où x, y et z sont des entiers naturels non nuls.

2°) Résoudre l'équation 7u +4v = 100 , u∈Z et v∈Z .

3°) Donner alors toutes les solutions du « Problème des cent volailles ».

Exercice 7 : Problème du « cuisinier chinois »

Il semble que l'appellation « cuisinier chinois » n'ait rien à voir avec une quelconque origine chinoise de ce problème. Mais on retrouve dans celui-ci une situation semblable à celles des exercices précédents, quoiqu'un peu plus compliquée : la mise en équation conduit à la résolution d'équations du type au + bv = 1 où a et b sont premiers entre eux.

Un équipage de dix-sept pirates disposant d'un butin composé de pièces d'or - supposées d'égale valeur - est d'accord sur le principe d'un partage égal entre ses membres, le reste revenant... au cuisinier chinois. Au départ celui-ci peut espérer trois pièces mais une querelle éclate, six pirates sont tués, le partage lui laisserait alors quatre pièces. Après la disparition de cinq autre pirates lors d'un naufrage ultérieur, il lui reviendrait cinq pièces. C'est alors qu'il décide d'empoisonner les survivants.

Quel butin minimum espère-t-il tirer de cette action ?

Exercice 8 : *Variante du problème précédent*

Un militaire en retraite a la charge de la formation de 180 majorettes. Pour leur apprendre à marcher au pas, il les fait défiler par 4 mais il y a une majorette en trop ; puis par 5, il y a cette fois 2 majorettes en trop ; enfin par 7, il en reste encore 3. Alors le militaire – qui a eu le loisir d'étudier le problème du « cuisinier chinois » en Indochine – s'écrie : « les 23 qui sont restées à la maison seront punies ! »

Expliquer le raisonnement du militaire, sachant qu'un simple coup d'œil lui apprend de façon évidente qu'il est en présence de beaucoup plus d'une vingtaine de jeunes filles.

4- Arithmétique et codes secrets

Vouloir communiquer avec un interlocuteur sans qu'une troisième personne puisse comprendre les messages échangés génère des problèmes aussi vieux que les premiers langages . Les solutions ou clefs, consistent à contrefaire un langage, et, s'il est écrit, à remplacer les lettres (ou les idéogrammes) par d'autres ayant la même signification aux yeux seuls du destinataire. Certaines de ces méthodes peuvent utiliser des propriétés de l'Arithmétique, mais les moyens techniques actuels rendent nécessaires l'élaboration de méthodes très avancées pour éviter tout décodage intempestif.

Ces méthodes sont donc numériques, d'où le nom de "Chiffrage" utilisé pour coder les messages et de "Service du Chiffre" pour désigner les structures mises en place par les différents pays pour coder et décoder les messages devant conserver une certaine confidentialité. Nous allons examiner quelques-unes de ces méthodes[6]

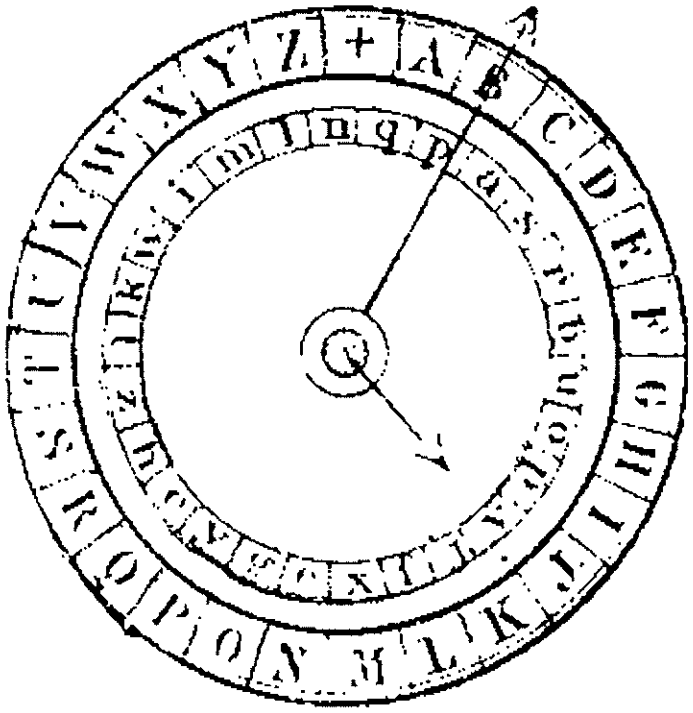
1. Très simple : la translation modulo 26

Ce système a été utilisé par Jules CESAR et porte souvent son nom. Il consiste à numéroter chaque lettre par sa place dans l'alphabet (A par 1, B par 2, C par 3, etc) et à la remplacer par la lettre correspondant à un numéro décalé d'une constante, soit:

Numéro de lettre codée = Numéro de lettre originale + constante (modulo 26)

« modulo 26 » signifie que lorsque le numéro de lettre codée dépasse 26, on retranche 26. Ce calcul, dit calcul "modulaire", peut se représenter par deux cercles concentriques, chacun gradué par les 26 lettres de l'alphabet; l'un des deux sera mobile et sa rotation suivant un certain angle correspondra à la constante de la translation.

[6] Nous renvoyons le lecteur intéressé au livre de Simon Singh « Histoire des codes secrets » publié chez JC Lattès.



Le cryptographe de Wheatstone (alphabet clair à l'extérieur, cryptographique à l'intérieur)

Exemple

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Prenons 10 pour valeur de la constante ; la lettre D (n°4) sera codée par la lettre portant le numéro 14, c'est-à-dire N, et la lettre Q (n°17) sera codée par la lettre portant le numéro 17+10-26 = 1, c'est-à-dire A.

Exercice 1 : Décoder le message suivant sachant qu'il a été codé avec le chiffre de César, la constante étant égale à 21 :

GZN MVXDIZN YZN HJON NJIO-ZGGZN XVMMZZN ? (Z. DJIZNXJ)

Ce système est élémentaire, mais aussi très simple à percer, puisqu'il suffit de déterminer la constante, en repérant par exemple un mot particulier.

2. Plus élaboré : la transformation affine

On peut compliquer la méthode de la façon suivante:

Numéro de lettre codée = a×(Numéro de lettre originale) + b (modulo 26) où a et b sont des constantes. Toutefois a doit être premier avec 26 sinon on risque d'avoir des lettres différentes codées par la même lettre.

Par exemple, prenons a = 2 et b = 5 :

M (n°13) sera codé par la lettre $2\times 13 + 5 = 26 + 5$ c'est-à-dire par la lettre E (n°5)

Z (n°26) sera codé par la lettre $2\times 26 + 5$ c'est-à-dire aussi par la lettre E (n°5)

De même,

O (n°15) sera codé par la lettre $2\times 15 + 5 = 26 + 9$ c'est-à-dire par la lettre I (n°9)

B (n°2) sera codé par la lettre $2\times 2 + 5 = 9$ c'est-à-dire aussi par la lettre I (n°9)

Avec a = 13 (et b = 5) toutes les lettres portant un numéro pair sont codées E et toutes celles portant un numéro impair sont codées R !

Plus généralement, deux lettres de numéros différents n et n' seront codées par la même lettre si, et seulement si :

$$\left|\begin{array}{lll} an+b \equiv an'+b \pmod{26} & \Leftrightarrow & an-an' \equiv 0 \pmod{26} \\ & \Leftrightarrow & a(n-n') = 26k \\ & \Leftrightarrow & 26 \textit{ divise } a(n-n') \end{array}\right.$$

Or, si 26 est premier avec a, alors 26 divise $(n\text{-}n')$ ce qui implique que $n=n'$ puisque $|n-n'| \leq 25$ .Donc, si 26 est premier avec a, deux lettres différentes seront codées par des lettres différentes.

Exercice 2 : En prenant a = 3 et b = 6 , coder le texte suivant :

« Nul ne sait ce qu'est une variable » (Hermann WEYL, l'un des plus grands mathématiciens du XXème siècle).

Cependant, percer le secret de ce code reste aussi facile que dans le premier cas ! Ces systèmes, arithmétiques ou non, qui consistent à substituer une lettre à une autre, voire par tout autre symbole, ne résistent pas à une analyse basée sur les fréquences reconnues des lettres.

Le mathématicien arabe Al Kindi (IXème siècle) s'était fait une spécialité du décryptage de ces systèmes. Ils furent cependant longtemps utilisés. Voilà ce qu'en dit Al Kindi dans son traité « Manuscrit sur le déchiffrement des messages cryptographiques » :

> Une façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Nous appellerons la lettre apparaissant le plus souvent la « première », la suivante la « deuxième », la suivante la « troisième », et ainsi de suite pour chaque lettre figurant dans le texte.
>
> Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et nous relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre « première » du texte clair, le suivant par la « deuxième », le suivant par la « troisième », et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre.

Appliquons cette méthode au texte suivant (il s'agit d'un texte en français) :

JPWKL KYXXLAKJWH J QL QLAHWB HBLQ PJQQL UL BLQHLB JQQWQL J KYHL UL QJ QYLRB QRB PL HJPRQ LH UL A'JIYWB BWLA J VJWBL : RAL VYWQ YR ULRN, LPPL JIIJWH OLHL RA KYRG U'YLWP QRB PL PWIBL ZRL QJ QYLRB PWQJWH, XJWQ WP AL KYAHLAJWH AW WXJMLQ, AW KYAILBQJHWYAQ.

PLCWQ KJBBYPP

On dresse la table des fréquences des lettres du texte :

Lettre	Fréquence (en %)	Lettre	Fréquence (en %)
A	6 ,31	N	0
B	7,28	O	0,48
C	0,48	P	6,80
D	0	Q	11,16
E	0	R	5,34
F	0	S	0
G	0,48	T	0
H	6,31	U	2,43
I	1,94	V	0,97
J	9,71	W	10,19
K	3,88	X	1,94
L	16,51	Y	6,31
M	0,48	Z	0,48

Et on la compare à la table suivante basée sur des textes provenant de journaux ou de romans, pour un échantillonnage d'environ 10 000 caractères :

Lettre	Fréquence (en %)	Lettre	Fréquence (en %)
A	9,42	N	7,15
B	1,02	O	5,14
C	2,64	P	2,86
D	3,39	Q	1,06
E	15,87	R	6,46
F	0,95	S	7,90
G	1,04	T	7,26
H	0,77	U	6,24
I	8,41	V	2,15
J	0,89	W	0
K	0	X	0,30
L	5,34	Y	0,24
M	3,24	Z	0,32

Dans le texte codé le L remplace vraisemblablement la lettre E du texte clair. Pour ce qui concerne la lettre Q, c'est moins évident : remplace-t-elle un I ? un N ? Pour trancher, c'est sa place dans les mots que l'on va considérer : dans le texte codé, Q est souvent redoublé, ce serait très étonnant qu'il remplace un I !

Exercice 3 : Continuez ainsi la comparaison des fréquences et décryptez ce texte. Le chiffre utilisé est-il basé sur le calcul modulaire ?

Un « bon chiffre » est évidemment un chiffre inviolable. De nombreuses et différentes méthodes ont été utilisées dans l'histoire, telle celle qui consiste à remplacer chaque lettre par celle occupant la même place dans une phrase donnée ou dans la page d'un certain livre : la clef ! Cependant il faut que le destinataire puisse lire le message, donc qu'il connaisse la clef; comme le moyen le plus sûr est d'utiliser une clef aussi longue que le message, la lecture en clair risque d'être laborieuse...L'utilisation d'une méthode numérique permettra le décodage rapide par le destinataire, voire par une machine, ce qui devient indispensable à l'époque où les messages deviennent de plus en plus nombreux et les moyens de transmissions performants.

Lors de la Seconde guerre mondiale, les Allemands ont utilisé des machines très perfectionnées, basées sur le calcul modulaire, pour coder leurs messages : les machines « Enigma ». Le Service du Chiffre anglais a employé jusqu'à 7000 personnes pour briser le chiffre d'Enigma et ses succès ont sans doute modifié le cours de la guerre.

L'apparition des ordinateurs a permis d'accélérer le décryptage et, de ce fait, a obligé les cryptanalystes à inventer des systèmes de codage de plus en plus compliqués. Nous allons en examiner deux exemples voisins dans leur principe.

3. Le codage par blocs :

Le principe est de regrouper par blocs les lettres du message original, en remplaçant chaque lettre par un nombre à 2 chiffres(A par 01...). Supposons que la longueur des blocs soit, pour faire simple, de 3. Prenons un nombre premier p supérieur à tout nombre à 3 chiffres obtenu par les blocs du message original et c (la clef, ou exposant de chiffrement) un nombre entier premier avec p-1. Pour chaque bloc, on procède au calcul:

(bloc codé)= (bloc original)^c (modulo p) , en conservant toujours des blocs à 3 chiffres, par exemple, en notant 003 pour 3.

Dans la pratique, on choisira une longueur de bloc la plus grande possible.

Exemple : Considérons le message suivant :

RENDEZ-VOUS VENDREDI SOIR

codé avec les numéros des lettres et découpé en blocs de trois chiffres:

170 413 030 425 211 420 182 104 130 317 040 308 181 408 173 (le dernier 3 a été rajouté au hasard pour compléter le dernier nombre à trois chiffres).

Choisissons p = 971 et c = 9 . On effectue le calcul indiqué plus haut sur chacun des blocs. Ainsi : $170^9 \equiv 71 \pmod{971}$, $413^9 \equiv 160 \pmod{971}$, etc..., ce qui donne :

071 160 852 585 721 076 079 150 949 642 920 651 194 503 035 .

Comment décoder un tel message ? Faisons d'abord un peu d'arithmétique.

On démontre, en arithmétique, que, si a et n sont premiers entre eux, alors a est **inversible modulo n**, c'est-à-dire qu'il existe b tel que $ab \equiv 1 \pmod{n}$.

Démonstration : a et n étant premiers entre eux, il existe b et c tels que ab + nc = 1 (Théorème de Bézout). Autrement dit, n divise 1-ab, ou encore $ab \equiv 1 \pmod{n}$

Ici c et p-1 sont premiers entre eux ; donc il existe d (l'exposant de déchiffrement) tel que $cd \equiv 1 \pmod{p-1}$. (Remarque : l'inverse de c modulo p-1 n'est pas unique, mais il existe un seul inverse compris entre 1 et p-1).

Par ailleurs, un corollaire du « Petit théorème de Fermat » dit que :

Pour tout entier a et tout nombre premier p, si $r \equiv 1 \pmod{p-1}$ *alors* $a^r \equiv a \pmod{p}$

Ici, puisque $cd \equiv 1 \pmod{p-1}$, alors, pour tout entier a, $(a^c)^d \equiv a^{cd} \equiv a \pmod{p}$.

Exemple (suite) : on doit d'abord déterminer d, l'exposant de déchiffrement. On doit donc trouver d tel que $9d \equiv 1 \pmod{970}$, ou encore trouver d et d' tels que 9d + 970d' = 1. On utilise l'algorithme d'Euclide et on trouve d =539 (et d' = -5). Et il ne reste plus qu'à calculer 71^{539}, 160^{539}, etc...pour retrouver 170, 413 et la suite des blocs initiaux.

Dans la pratique, lorsque deux personnes veulent utiliser ce chiffrement pour échanger des messages elles doivent se mettre d'accord sur un triplet (p, c, d) où p est un nombre premier, c un

nombre premier avec p-1, et d l'inverse de c modulo p-1. Le couple (p, c) ne doit pas être divulgué, sinon il est alors facile de calculer d : c'est un chiffrement **à clef secrète**. Se pose donc le problème de la transmission de la clef entre les deux correspondants : s'ils habitent dans la même région on peut envisager qu'ils se rencontrent pour échanger cette clef, mais la plupart du temps les échanges de messages se font entre des individus qui sont dans l'impossibilité de se rencontrer et il faudrait trouver un moyen sûr de transmettre la clef. Des chercheurs américains ont mis au point un système tout à fait génial : un chiffrement **à clef publique.**

4. Le système RSA : *(les lettres R S et A sont les initiales des trois chercheurs Rivest, Shamir et Adleman qui ont mis au point ce système en 1977)*

Le principe repose sur les résultats d'arithmétique cités dans l'exemple précédent : « si a et n sont premiers entre eux alors a est inversible modulo n », et le corollaire du petit théorème de Fermat. Mais toute l'astuce consiste dans le choix de n. Voyons cela de plus près.

Imaginons que Antoine veuille recevoir un message de Béatrice **que personne d'autre que lui ne puisse lire.**

Il choisit deux nombres premiers très grands p et q (à 50 chiffres par exemple) ; il calcule leur produit n = pq ainsi que le produit m = (p-1)(q-1). Puis il choisit un nombre c premier avec m, compris entre 2 et m-2, et enfin il calcule d l'inverse de c modulo m. Il envoie à Béatrice la clef (n , c), qui peut être interceptée par n'importe qui, cela n'a aucune importance, et garde pour lui (n , d). En effet, puisque n est très grand, il est pratiquement impossible de le décomposer en facteurs premiers[7] et il est donc impossible de trouver m et d.

Béatrice veut envoyer un message à Antoine. Elle commence par le transformer en un nombre, par exemple en remplaçant les lettres par leur numéro. Soit M ce nombre. Elle calcule (avec son ordinateur !) le nombre $C \equiv M^c \pmod{n}$ et envoie C à Antoine. Celui-ci calcule $C' \equiv C^d \equiv M^{cd} \equiv M \pmod{n}$ et il ne lui reste plus qu'à le retranscrire en lettres.

Tout ceci nécessite évidemment des outils de calcul performants et l'exemple concret que nous vous proposons est un peu simpliste mais il va permettre de mieux saisir le principe.

Exemple : Antoine a choisi p = 13 et q = 17, a calculé n =13×17 = 221, puis choisit c = 5. Il rend publique la clef (221, 5). Il calcule par ailleurs l'inverse de 5 modulo m (où m = 12×16 =192) et trouve d = 77 **mais garde ce nombre secret**.

Béatrice veut envoyer le message NON à Antoine. Elle code ce message par le nombre 141514 qu'elle découpe en blocs de 2 chiffres (pour simplifier les calculs) : 14 15 14 (voir le codage par blocs). Puis elle élève chacun des nombres ainsi formés à la puissance 5 et obtient, en utilisant les congruences modulo 221 : 131 19 131, message qu'elle envoie à Antoine.

Antoine calcule alors 131^{77} et 19^{77} et retrouve alors le message 14 15 14 qu'il peut enfin transcrire en clair : NON.

Exercice 4 : Boris et Anton jouent aux échecs et ont l'habitude de se communiquer des « coups » de façon confidentielle. Par exemple, le « coup » B3 → D4 sera transformé en la suite de nombres 23 44 avant d'être codé par le système RSA. Anton a donné la clé suivante à Boris : (33 , 3). Boris lui envoie le message codé suivant : 5 23.

Trouver la clé de décodage d (ici ce n'est pas difficile car 33 n'est pas un grand nombre !).

Trouver le « coup » indiqué par Boris.

[7] Voir le chapitre sur les nombres premiers et les tests de primalité. Le record actuel de factorisation est de 120 chiffres et nécessite de faire travailler un ordinateur très puissant pendant un mois. C'est pourquoi RSA est considéré comme un système inviolable dès lors qu'on utilise des grands nombres premiers.

Statue de Fermat à Toulouse

Fermat et sa muse

ANNEXE 1

1. Les nombres de Fermat

Les nombres de Fermat sont les nombres de la forme $2^{2^n}+1$ où n est un entier non nul. Fermat pensait que de tels nombres étaient tous premiers ; cela est vrai pour n = 1, 2, 3, 4 mais Euler a établi en 1732 que $2^{2^5}+1$ ne l'est pas.

En effet $2^{2^5}+1 = 4\,294\,967\,297 = 641 \times 6\,700\,417$

On sait actuellement (août 2000) que $2^{2^n}+1$ n'est pas premier pour $5 \le n \le 30$ et on pense que, à part les cas n = 1, 2, 3, 4, il n'existe pas d'autres nombres premiers de la forme $2^{2^n}+1$.

Voici ci-dessous la liste de certains facteurs premiers de la décomposition des nombres de Fermat pour $1 \le n \le 16$, ainsi que les noms des mathématiciens les ayant découverts. Il est à noter qu'on connaît la décomposition complète en facteurs premiers seulement pour n = 5, 6, 7, 8, 9, 10 et 11. Pour d'autres on ne connaît qu'un facteur premier (par exemple pour n = 15) ou même aucun, bien qu'on sache qu'il s'agit d'un nombre composé (par exemple pour n = 14, 20, 22, 24[1]).

[1] Le 24ième nombre de Fermat s'écrit avec plus de cinq millions de chiffres. R.Crandall et ses collègues du *Center for Advanced Computation* à Portland ont montré, en 1999, qu'il était composé.

n	Facteurs premiers	Date	Découvert par
1	5		Fermat
2	17		Fermat
3	257		Fermat
4	65537		Fermat
5	641	1732	Euler
5	6 700 417	1732	Euler
6	274 177	1880	Landry
6	67 280 421 310 721	1880	Landry, Le Lasseur, Gérardin
7	59 649 589 127 497 217	1970	Morrison, Brillhart
7	5 704 689 200 685 129 054 721	1970	Morrison, Brillhart
8	1 238 926 361 552 897	1909	Morehead, Western
9	2 424 833	1903	Western
9	Décomposition complète	1967	Brillhart
10	45 592 577	1953	Selfridge
10	6 487 031 809	1962	Brillhart
10	455 925 777	1967	Brillhart
11	319 489	1899	Cunningham
11	974 849	1899	Cunningham
12	114 689	1877	Lucas, Pervouchine
12	26 017 793	1903	Western
12	63 766 529	1903	Western
12	190 274 191 361	1974	Hallyburton, Brillhart
13	2 710 954 639 361	1974	Hallyburton, Brillhart
14	Composé (facteurs inconnus)	1961	Selfridge, Hurwitz
15	1 214 251 009	1925	Kraitchik
16	825 753 601	1953	Selfridge

2. Les nombres de Mersenne

Les nombres de Mersenne sont les nombres de la forme $2^n - 1$ où n est un entier non nul. Certains sont premiers, d'autre non. On connaît actuellement (août 2000) 38 nombres de Mersenne premiers. Voici la liste des nombres de Mersenne premiers pour $2 \leq n \leq 250$:

n	$M = 2^n - 1$
2	3
3	7
5	31
7	127
13	8 191
17	131 071
19	524 287
31	2 147 483 647
61	2 305 843 009 213 693 951
89	618 970 019 642 690 137 449 562 111
107	162 259 276 829 213 363 391 578 010 288 127
127	170 141 183 460 469 231 731 687 303 715 884 105 727

Les vingt-six autres nombres premiers de Mersenne connus sont ceux correspondant à n = 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593. Les sept derniers de cette liste font partie du « Top Ten » des plus grands nombres premiers connus.

3. Les records

Même si l'ordinateur permet plus aisément de faire des calculs, les « plus grands nombres premiers » sont, depuis toujours, le résultat de l'intelligence et de l'innovation.

Voici par exemple la liste des plus grands nombres premiers obtenus sans l'aide d'un ordinateur :

Nombre	Nombre de chiffres	Découvert par	Date	Méthode
$2^{17}-1$	6	Cataldi	1588 (?)	Division
$2^{19}-1$	6	Cataldi	1588 (?)	Division
$2^{31}-1$	10	Euler	1772 (?)	Division et raisonnement
$\frac{2^{59}-1}{179951}$	13	Landry	1867	Division et raisonnement
$2^{127}-1$	39	Lucas	1876	Suite de Lucas
$\frac{2^{148}+1}{17}$	44	Ferrier	1951	Théorème de Proth

● Les dix plus grands nombres premiers connus (août 2000)[2] :

Nombre	Nombre de chiffres	Découvert par	Date
$2^{6972593} - 1$	2 098 960	Hajratwala, Woltman, Kurowski, GIMPS	1999
$2^{3021377} - 1$	909 526	Clarkson, Woltman, Kurowski, GIMPS	1998
$2^{2976221} - 1$	895 932	Spence, Woltman, GIMPS	1997
$2^{1398269} - 1$	420 921	Armengaud, Woltman, GIMPS	1996
$2^{1257787} - 1$	378 632	Slowinski,Gage	1996
$48594^{65536} + 1$	307 140	Scott, Gallot	2000
$2^{859433} - 1$	258 716	Slowinski,Gage	1994
$2^{756839} - 1$	227 832	Slowinski,Gage	1992
$167176^{32768} + 1$	171 153	Gallot	2000
$169719.2^{557557} + 1$	167 847	Scott, Gallot	2000

Le 1er Juin 1999 l'équipe de Hajratwala, Woltman, Kurowski a découvert le 38ème nombre de Mersenne premier (il se peut qu'il existe d'autres nombres de Mersenne

[2] Cette liste évolue rapidement !

premiers inférieurs à celui-ci car les exposants précédents n'ont pas tous été essayés). Hajratwala fait partie, ainsi qu'environ 12 000 personnes dans le monde, du réseau GIMPS (the Great Internet Mersenne Prime Search) créé par Woltman au début de 1996. GIMPS fournit un logiciel gratuit aux possesseurs d'ordinateurs personnels destiné à la recherche des grands nombres premiers.

Il a fallu 111 jours à Hajratwala, sur son ordinateur personnel, un Aptiva 350 MHz, pour trouver ce nombre. Si son ordinateur avait tourné jour et nuit cela aurait pris trois semaines.

●Les dix plus grands nombres premiers jumeaux connus (août 2000)[3]

Nombre	Nombre de chiffres	Découvert par	Date
$4648619711505.2^{60000}\pm1$	18 075	Indlekofer, Jarai, Wassing	2000
$2409110779845.2^{60000}\pm1$	18 075	Indlekofer, Jarai, Wassing	2000
$2230907354445.2^{48000}\pm1$	14 462	Indlekofer, Jarai, Wassing	1999
$871892617365.2^{48000}\pm1$	14 462	Indlekofer, Jarai, Wassing	1999
$361700055.2^{39020}\pm1$	11 755	Lifchitz	1999
$835335.2^{39014}\pm1$	11 751	Ballinger, Gallot	1998
$242206083.2^{38880}\pm1$	11 713	Indlekofer, Jarai	1995
$40883037.2^{23456}\pm1$	7 069	Lifchitz, Gallot	1998
$843753.2^{22222}\pm1$	6 696	Rivera, Gallot	1997
$9219177.2^{20202}\pm1$	6 089	Narayanan, Gallot	2000

[3] Voir note ci-dessus.

4. Les nombres parfaits :

Ce sont des nombres égaux à la somme de leurs diviseurs propres ; ils sont de la forme $2^p(2^{p+1}-1)$. En voici la liste des 30 premiers :

Nombre	Nombre de chiffres	Découvert par	Date
$6 = 2(2^2-1)$	1	Connu d'Euclide	?
$28 = 2^2(2^3-1)$	2	Connu d'Euclide	?
$496 = 2^4(2^5-1)$	3	Connu d'Euclide	?
$8128 = 2^6(2^7-1)$	4	Connu d'Euclide	?
$33\,550\,336 = 2^{12}(2^{13}-1)$	8	inconnu	1456
$8\,589\,869\,056 = 2^{16}(2^{17}-1)$	10	Cataldi	1588
$137\,438\,691\,328 = 2^{18}(2^{19}-1)$	12	Cataldi	1588
$2^{30}(2^{31}-1)$	19	Euler	1772
$2^{60}(2^{61}-1)$	37	Pervouchine	1883
$2^{88}(2^{89}-1)$	54	Powers	1911
$2^{106}(2^{107}-1)$	65	Powers	1914
$2^{126}(2^{127}-1)$	77	Lucas	1876
$2^{520}(2^{521}-1)$	314	Robinson	1952
$2^{606}(2^{607}-1)$	366	Robinson	1952
$2^{1278}(2^{1279}-1)$	770	Robinson	1952
$2^{2202}(2^{2203}-1)$	1327	Robinson	1952
$2^{2280}(2^{2281}-1)$	1373	Robinson	1952
$2^{3216}(2^{3217}-1)$	1937	Riesel	1957
$2^{4252}(2^{4253}-1)$	2561	Hurwitz	1961
$2^{4422}(2^{4423}-1)$	2663	Hurwitz	1961
$2^{9688}(2^{9689}-1)$	5834	Gillies	1963
$2^{9940}(2^{9941}-1)$	5985	Gillies	1963
$2^{11212}(2^{11213}-1)$	6751	Gillies	1963
$2^{19936}(2^{19937}-1)$	12003	Tuckerman	1971
$2^{21700}(2^{21701}-1)$	13066	Nickel et Noll	1978
$2^{23208}(2^{23209}-1)$	13973	Noll	1979
$2^{44496}(2^{44497}-1)$	26790	Nelson et Slowinski	1979
$2^{86242}(2^{86243}-1)$	51924	Slowinski	1982
$2^{110502}(2^{110503}-1)$	66530	Colquitt et Welsh	1988
$2^{132048}(2^{132049}-1)$	79502	Colquitt et Welsh	1991

On ne sait pas s'il existe des nombres parfaits entre ceux qui correspondent à p=132 048 et à p=216 090

5. Des formules pour trouver des nombres premiers :

La quête d'une formule pour trouver des nombres premiers en est à ses débuts. On peut toutefois signaler :

la formule d'Euler $P(n) = n^2 - n + 41$ *pour* $1 \le n \le 107$ qui donne un nombre premier dans 47,5% des cas ($P(n)$ est premier pour $1 \le n \le 40$) ;

les formules de Ulam (mathématicien contemporain d'origine polonaise) :

$4n^2 + 170n + 1847$ (pourcentage de réussite 46,6%) qui permet d'engendrer 760 nombres premiers non obtenus par la formule d'Euler ;

$4n^2 + 4n + 59$ (pourcentage de réussite 43,7%) qui donne 1500 nombres premiers non obtenus par les formules précédentes ;

la formule de Hardy (1ère moitié du XXème siècle) :

pour tout entier N, le plus grand facteur premier H(N) de N est

$$H(N) = \lim_{r\to+\infty} \lim_{m\to+\infty} \lim_{n\to+\infty} A(r,m,n) \quad où \quad A(r,m,n) = \sum_{i=0}^{m} \left[1 - \left(\cos \frac{(i!)^r \pi}{N} \right)^{2n} \right]$$

… mais cette formule n'a aucun intérêt pratique !

ANNEXE 2

Pour déterminer si un nombre n est premier, le moyen le plus simple est le crible d'Eratosthène ou les divisions successives par les nombres premiers inférieurs à $\sqrt{n}$; mais ces procédés ne conviennent pas pour des nombres comportant plusieurs dizaines de chiffres.

99,9% des nombres de la liste des « plus grands nombres premiers » ont été trouvés grâce aux tests de Lucas et de Pépin ou à des versions améliorées de ceux-ci, plus performantes.

Il existe aussi des tests probabilistes, c'est-à-dire des tests qui permettent de dire qu'un nombre a une forte probabilité d'être premier. Essayons d'en expliquer le principe.

Rappelons que le théorème de Fermat permet d'affirmer qu'un nombre p est composé mais que sa réciproque est fausse. Ainsi 341 est composé bien que 341 vérifie la conclusion du théorème de Fermat en prenant a $= 2$: on dit alors que 341 est « pseudo-premier de base 2 ». Voici d'autres exemples de nombres pseudo-premiers :

91 est pseudo-premier de base 3 (91 divise $3^{90} - 1$)

217 est pseudo-premier de base 5 (217 divise $5^{216} - 1$)

25 est pseudo-premier de base7 (25 divise $7^{24} - 1$)

Les nombres pseudo-premiers, bien qu'en quantité infinie sont rares. Ainsi il existe un peu plus d'un million de nombres premiers inférieurs à 25.10^9 mais seulement 21853 pseudo-premiers de base 2 et 1770 pseudo-premiers à la fois pour les bases 2, 3, 5 et 7. Les tests probabilistes consistent à choisir des nombres premiers $a_1, a_2, \cdots, a_k$ qui serviront de base. On considère un nombre entier N dont on veut savoir s'il est premier ou non ; si ce nombre vérifie la conclusion du théorème de Fermat avec chacun des a_i, c'est-à-dire que, pour tout i, N divise $a_i^{N-1} - 1$, alors N est pseudo-premier de base $a_1, a_2, \cdots, a_k$. Il y a donc une forte probabilité que N soit premier. Mais il se peut aussi qu'on ait affaire à un nombre appelé « nombre de Carmichael ».Un nombre composé est dit « de Carmichael » si, pour tout entier a premier avec n, n divise $a^{n-1} - 1$. Bien que ces nombres soient rares (il en existe 2163 inférieurs à 25.10^9) on a montré récemment qu'il y en a une infinité. Les nombres de Carmichael inférieurs à 100 000 sont :

561, 1 105, 1 729, 2 465, 2 821, 6 601, 8 911, 10 585, 15 841, 29 341, 41 041, 46 657, 52 633, 62 745, 63 973 et 75 361.

D'autres tests probabilistes plus récents (test d'Adelman, Pomerance et Rumely (1983)) s'appuient sur le théorème d'Euler :

a et p étant premiers entre eux, si p est premier alors p divise $a^{p-1/2} - 1$.

La réciproque de ce théorème est, elle aussi, fausse ; on appelle nombre « pseudo-premier fort de base a » tout nombre p composé vérifiant la conclusion du théorème d'Euler. En voici quelques-uns :

2047 est pseudo-premier fort de base 2

121 est pseudo-premier fort de base 3

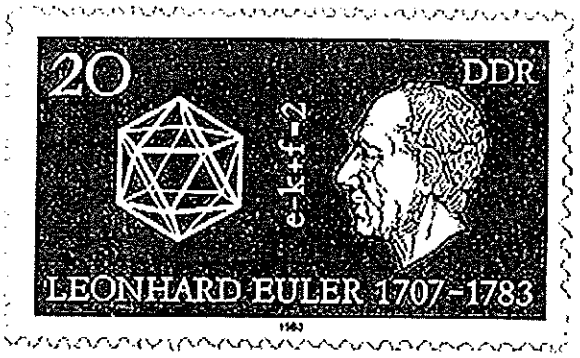
781 est pseudo-premier fort de base 5

25 est pseudo-premier fort de base 7

Les nombres pseudo-premiers forts sont extrêmement rares, bien qu'eux aussi en nombre infini. On a ainsi établi que

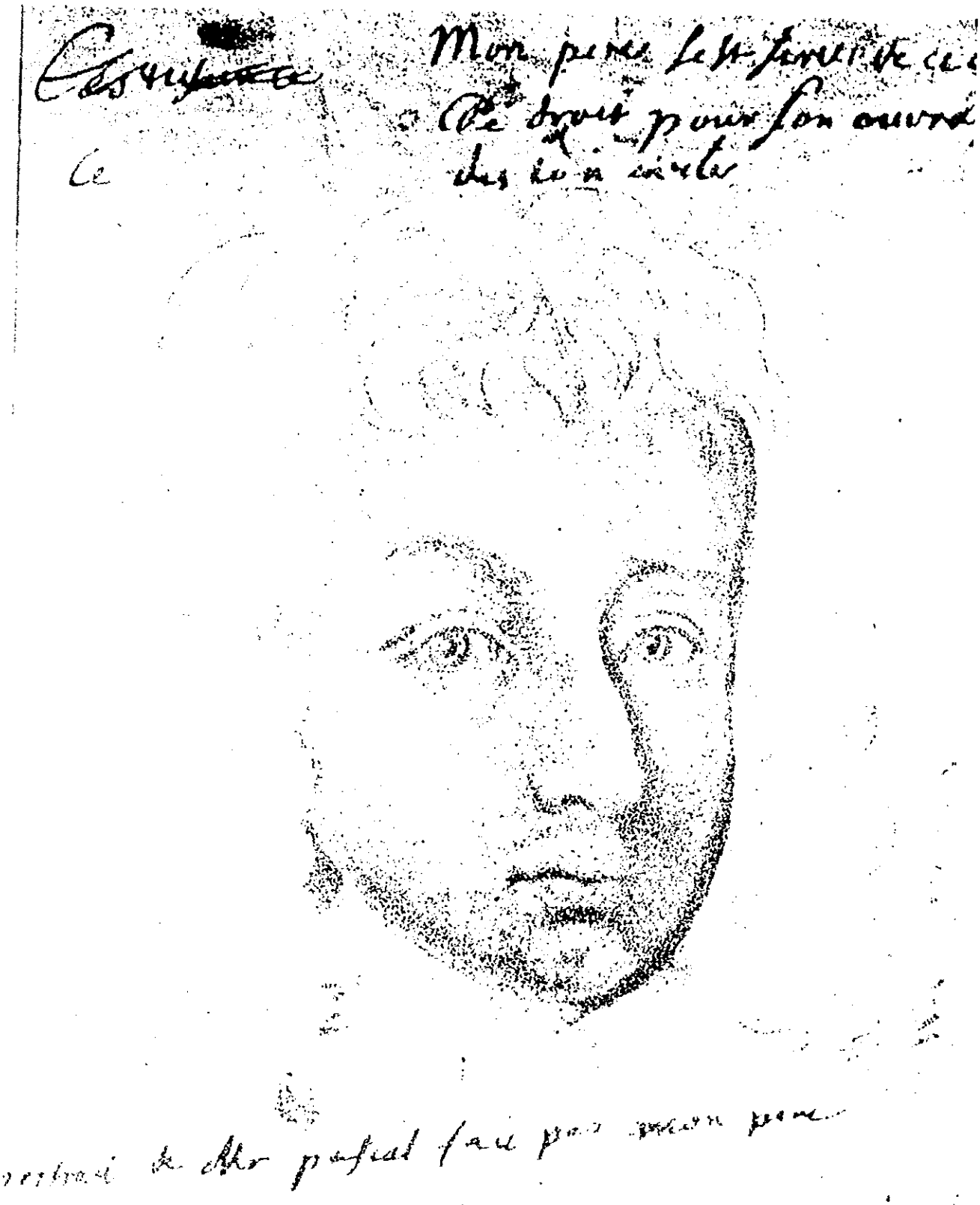
si $n < 1\ 373\ 653$ est pseudo-premier fort de base 2 et 3, alors n est premier ;

si $n < 3\ 474\ 749\ 660\ 383$ est pseudo-premier fort de base2, 3, 5, 7, 11 et 13 alors n est premier.



ANNEXE 3

Pascal jeune, portrait à la sanguine par Jean Domat



Des caractères de divisibilité des nombres déduits de la somme de leurs chiffres

Pascal, œuvres complètes, éditions du seuil, Paris, 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 quantités 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.

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

Annexe 4

Les mille premiers nombres premiers

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
53	59	61	67	71	73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173	179	181	191	193	197
199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379
383	389	397	401	409	419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541	547	557	563	569	571
577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941	947	953	967	971	977
983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187
1193	1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399	1409	1423	1427
1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613
1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867
1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087
2089	2099	2111	2113	2129	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287	2293	2297	2309	2311	2333
2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557
2579	2591	2593	2609	2617	2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741	2749	2753	2767	2777	2789
2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037
3041	3049	3061	3067	3079	3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271	3299	3301	3307
3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539
3541	3547	3557	3559	3571	3581	3583	3593	3607	3613	3617	3623	3631	3637	3643

3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769
3779 3793 3797 3803 3821 3823 3833 3847 3851 3853 3863 3877 3881 3889 3907
3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001 4003 4007 4013 4019
4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139
4153 4157 4159 4177 4201 4211 4217 4219 4229 4231 4241 4243 4253 4259 4261
4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373 4391 4397 4409
4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523
4547 4549 4561 4567 4583 4591 4597 4603 4621 4637 4639 4643 4649 4651 4657
4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787 4789 4793
4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937
4943 4951 4957 4967 4969 4973 4987 4993 4999 5003 5009 5011 5021 5023 5039
5051 5059 5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171 5179
5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323
5333 5347 5351 5381 5387 5393 5399 5407 5413 5417 5419 5431 5437 5441 5443
5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527 5531 5557 5563 5569
5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693
5701 5711 5717 5737 5741 5743 5749 5779 5783 5791 5801 5807 5813 5821 5827
5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939
5953 5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091
6101 6113 6121 6131 6133 6143 6151 6163 6173 6197 6199 6203 6211 6217 6221
6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329 6337
6343 6353 6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473
6481 6491 6521 6529 6547 6551 6553 6563 6569 6571 6577 6581 6599 6607 6619
6637 6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761
6763 6779 6781 6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871
6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971 6977 6983 6991 6997
7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151
7159 7177 7187 7193 7207 7211 7213 7219 7229 7237 7243 7247 7253 7283 7297
7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433 7451 7457 7459
7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561
7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687
7691 7699 7703 7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829
7841 7853 7867 7873 7877 7879 7883 7901 7907 7919

François Edouard Anatole Lucas

Eratosthène

Joseph Louis Lagrange

Andrew Wiles

Sophie Germain

Euclide

Eléments de corrigés des questions et exercices :

Chapitre 1

I

Question 1 :

1 n'est pas un nombre, car un nombre est "une multitude d'unités".
(on notera que cette façon de comprendre le "1" perdurera assez longtemps, de façon plus ou moins affirmée.)

Question 2 :

"mesurer" signifie "diviser". Cela correspond bien au fait que l'on reporte un segment dans un autre un nombre entier exact de fois.

Question 3 :

14 vaut deux tiers de 21, donc deux "parties" qui sont chacune un "tiers".

Nous dirions : 7 divise 21, car $21 = 3 \times 7$, ou bien : $7 = \frac{21}{3} = \frac{1}{3} \times 21$

14 ne divise pas 21, car $21 = 1 \times 14 + 7$.

Question 4 :

Un nombre est multiple d'un autre, si la division du premier par le deuxième "tombe juste", c'est à dire qu'il n'y a pas de reste.
On reporte un nombre entier exact de fois le deuxième dans le premier.
Exemple : 15 est multiple de 3 , car $15 = 5 \times 3$, ou encore : $15 : 3 = 5$

Mais 17 n'est pas multiple de 3 car $17 = 5 \times 3 + 2$. La division ne tombe pas "juste". Il y a un reste égal à 2.

III

Question 1 :

Dans les deux propositions, on cherche combien de fois AB contient CD, par exemple n_1 fois, et il reste R_1 $(0 < R_1 < CD)$.

$AB = \overbrace{n_1 CD}^{BF} + \overbrace{R_1}^{FA}$ $\quad 0 < FA < BF.$

On continue en cherchant combien de fois R1 est contenu dans CD.

$CD = \overbrace{n_2 R_1}^{DG} + \overbrace{R_2}^{CG}$ $\quad 0 < CG < DG$

$DG = \overbrace{n_3 CG}^{FH} + \overbrace{AH}^{1}.$

En continuant, on arrive au dernier reste 1.

Si AB et CD ne sont pas premiers entre eux, un nombre (différent de 1) les mesure ; par exemple E.

E mesure (c'est à dire divise) AB et CD, donc aussi BF, donc AB - BF = FA.

E divise CD et FA donc CD et DG donc CD - DG = CG.

E divise DG et CG donc DG et FH donc DG - FH = AH = 1.

Pour nous, ceci signifie que E = 1, dans les deux cas.

Euclide distingue les deux propositions, car "1" n'est pas un nombre.

Question 2 : voir question 1.

Question 3 : *(n_1 est le nombre de fois que l'on a retranché B de A, c'est évidemment un entier).*

$A = n_1 B + R_1$

$B = n_2 R_1 + R_2$

$R_1 = n_3 R_2 + R_3$

...

$R_{p-2} = n_p R_{p-1} + R_p$

$R_{p-1} = n_{p+1} R_p$

Le PGCD (plus grand diviseur commun)[18].est la plus grande commune mesure. Si la plus grande commune mesure est 1, les nombres sont premiers entre eux.

[18] La raison de la dénomination PGCD pour "plus grand diviseur commun" est assez controversée. Logiquement les français devraient dire PGDC.

Question 4 :

$1463 = 5 \times 285 + 38$

$285 = 7 \times 38 + 19$

$38 = 2 \times 19 + 0$ (Euclide n'écrit pas bien sûr "+ 0" puisque le nombre 0 n'existe pas à son époque.)

Le PGCD de 1463 et de 38 est 19.

$65 = 1 \times 42 + 23$

$42 = 1 \times 23 + 19$

$23 = 1 \times 19 + 4$

$19 = 4 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0$

65 et 42 sont premiers entre eux.

IV

Question 1 :

La suite des restes est une suite décroissante de nombres entiers. Cette suite n'est donc pas illimitée et un des restes, le dernier, est obligatoirement nul.

Question 2 :

Si d divise a et b, alors il divise a et bq_1, donc $a - bq_1 = r_1$, donc d divise b et r_1.

Si d divise b et r_1, alors il divise $bq_1 + r_1$, donc a ; donc d divise a et b.

Ainsi, $D(a , b) = D(b , r_1)$.

De même, $D(b , r_1) = D(r_1 , r_2) = \ldots = D(r_{n-1} , r_n)$.

Or si d divise r_n alors d divise $r_n q_{n+1}$, donc r_{n-1}.

Donc $D(r_n) = D(r_{n-1} , r_n)$.

Question 3 :

r_n est le plus grand diviseur de $D(r_n)$, donc de $D(a , b)$.

Exercice :

PGCD de 1100005423 et de 1100000077.

$1100005423 = 1 \times 1100000077 + 5346$
$1100000077 = 205761 \times 5346 + 1771$
$5346 = 3 \times 1771 + 33$
$1771 = 53 \times 33 + 22$
$33 = 1 \times 22 + 11$
$22 = 2 \times 11 + 0$

Le PGCD de 1100005423 et de 1100000077 est 11.

Chapitre II

I

Question 1 :

Actuellement : un nombre est premier s'il admet comme seuls diviseurs 1 et lui-même. La différence vient du fait que 1 n'est pas un nombre pour Euclide.

Question 2 :

a) Si A, B, C sont des nombres premiers, A.B.C est le plus petit multiple commun (PPCM) de A, B et C.
b) $EF = A \times B \times C + DF = DE + DF$
c) Tout nombre non premier admet au moins un diviseur premier.
d) Soit G un nombre premier divisant EF, alors si G est un des nombres A, B ou C, il divise EF et DE donc aussi DF. Donc il divise 1. Ce qui est impossible pour Euclide ; ce qui signifie pour nous que c'est 1 ; donc il ne serait pas premier; donc ce ne peut être A, ni B, ni C.

Ainsi, ou bien EF est un nouveau nombre premier, ou bien il admet un diviseur premier qui n'est aucun de ceux connus auparavant, donc c'est un nouveau nombre premier.

e) L'ensemble des nombres premiers est donc infini, car quels que soient ceux que l'on connaît, on peut toujours en trouver un nouveau.

Le mot "infini" n'est pas un mot utilisé dans le vocabulaire grec. On préfère dire que l'on peut continuer indéfiniment la liste des nombres premiers.
Il s'agit d'un aspect de la philosophie qui fait la différence entre "l'infini en acte", et l'infini potentiel".

Question 3 :

$N = (2 \times 3 \times 5 \times 7 \times \ldots \times p) + 1$.
Si N est premier, alors nous avons trouvé un nombre premier supérieur à tous ceux utilisés.
Si N n'est pas premier, alors il possède au moins un diviseur premier q. q ne peut être aucun de ceux cités, sinon, comme dans la démonstration d'Euclide, il diviserait le produit
$2 \times 3 \times 5 \times 7 \times \ldots \times p$ et N, donc 1 et serait donc égal à 1, donc ne serait pas premier.
Nous avons donc un nouveau nombre premier q.

Question 4 :

$N = n ! + 1$.
Si N est premier, nous avons trouvé un nouveau nombre premier supérieur à n.
Si N n'est pas premier, il possède au moins un diviseur premier. Si ce diviseur est inférieur ou égal à n, il est un des facteurs de n !, donc il divise n ! et n, donc 1. Il est donc égal à 1 ce qui est impossible. Donc c'est un nombre supérieur à n.
Dans tous les cas, quel que soit n on peut trouver un nombre premier supérieur à n.

Question 5 :

Si $x = 5000$ $\quad \pi(x) = 669$ et $\dfrac{5000}{\ln 5000} \approx 587,05$

Si $x = 7000$ $\quad \pi(x) = 900$ et $\dfrac{7000}{\ln 7000} \approx 790,63$

Si $x = 7900$ $\quad \pi(x) = 997$ et $\dfrac{7900}{\ln 7900} \approx 880,26$

Question 6 :

$2^{2^1} + 1 = 5$

$2^{2^2} + 1 = 17$

$2^{2^3} + 1 = 257$

$2^{2^4} + 1 = 65537$

$2^{2^5} + 1 = 4294967297$

Les quatre premiers nombres de Fermat sont premiers.
Par contre 4294967297 est divisible par 641.

Question 7 :

$31 = 2^5 - 1$ est un nombre premier.

$63 = 2^6 - 1$ n'est pas premier;

Question 8 :

$2047 = 2^{11} - 1$, et 2047 n'est pas premier.

$131071 = 2^{17} - 1$ et 131071 n'est pas premier. (Il est divisible par 3).

Question 9 :

1319 et 1321
2129 et 2131

Question 10 :

a) $D(496) = \{1, 2, 4, 8, 16, 31, 62, 124, 248, 496\}$

Et $1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 496$

b) par exemple 6. Car les diviseurs de 6 sont 1, 2, 3 et 6 ; et $6 = 1 + 2 + 3$.

Question 11 :

a) $1+2+2^2+2^3+...+2^p = \dfrac{1-2^{p+1}}{1-2} = 2^{p+1} - 1$

b) $2^p(1+2+...+2^p) = 2^p(2^{p+1}-1)$

Si $2^{p+1} - 1$ est premier, les diviseurs de $A = 2^p(2^{p+1} -1)$ sont :

$1, 2, 2^2, ...2^p, 2^{p+1} - 1, 2(2^{p+1} -1), ..., 2^{p-1}(2^{p+1} -1)$.

Et la somme de ces diviseurs est : $1 + 2 + ... + 2^p + (2^{p+1} -1)(1 + 2 +.. + 2^{p-1})$

$= 2^{p+1} - 1 + (2^{p+1} - 1)(2^p - 1)$

$= (2^{p+1} - 1)(1 + 2^p - 1) = 2^p (2^{p+1} -1) = A$

II

Exercice :

Remarque : dans ce corrigé on a utilisé les congruences par commodité de rédaction ; la notion de congruence est présentée dans le chapitre suivant.

1°)341 n'étant pas divisible ni par 2, ni par 3 est donc premier avec chacun de ces nombres.

2°)

$3^{10} = 59049 = 341 \times 173 + 56$ donc $3^{10} \equiv 56 (\text{mod } 341)$

$56^3 = 175616 = 341 \times 515 + 1$ donc $56^3 \equiv 1 (\text{mod } 341)$

par conséquent $3^{30} \equiv 1 (\text{mod } 341)$

or $3^{340} = (3^{30})^{10} \times 3^{30} \times 3^{10}$, donc $3^{340} \equiv 56 (\text{mod } 341)$

et $3^{340} - 1$ a donc pour reste 55 dans la division par 341

341 ne divise pas $3^{340} - 1$: 341 nest pas premier.

3°) $2^{10} = 1024 = 341 \times 3 + 1$ donc $2^{10} \equiv 1 (\text{mod } 341)$

par conséquent $2^{340} \equiv 1 (\text{mod } 341)$

donc 341 divise $2^{340} - 1$ bien qu' il ne soit pas premier ! .

Chapitre 3

I

Ex 1

$3^4 = 81 = 2 \times 34 + 13$ donc $3^4 \equiv 13 (\text{mod } 34)$

par conséquent $3^8 \equiv 169$ et $169 = 5 \times 34 - 1$ donc $3^8 \equiv -1 \pmod{34}$
d'où il découle que $3^{16} \equiv 1 \pmod{34}$.
Par ailleurs $1604 = 16 \times 100 + 4$
Donc $3^{1604} \equiv 3^4 \equiv 13 .(\text{mod } 34)$
Le reste de la division de 3^{1604} par 34 est donc égal à 13.

Ex 2 :

$2^6 = 64 = 5 \times 13 - 1$ donc $2^6 \equiv -1 \pmod{13}$
donc $2^{12} \equiv 1 \pmod{13}$ or $70 = 5 \times 12 + 10$ donc $2^{70} = (2^{12})^5 \times 2^{10}$
et $2^{70} \equiv 2^{10} \pmod{13}$
Par ailleurs $2^{10} = 1024 = 79 \times 13 - 3$ donc $2^{70} \equiv -3 \pmod{13}$;
De même $3^3 \equiv 1 \pmod{13}$ et comme $70 = 23 \times 3 + 1$ alors $3^{70} = (3^3)^{23} \times 3$
Conclusion : $2^{70} + 3^{70} \equiv -3 + 3 \equiv 0 \pmod{13}$
Ce qui signifie que 13 divise la somme $2^{70} + 3^{70}$.

Ex 3 :

1° $5^4 = 625 = 641 - 16$ donc $5^4 \equiv -16 \pmod{641}$ et $-16 = -2^4$ d'où $5^4 \equiv -2^4 \pmod{641}$ (1).
$5 \times 2^7 = 640 = 641 - 1$ donc $5 \times 2^7 \equiv -1 \pmod{641}$ (2).
2° $2^{32} = 2^{28} \times 2^4$ et $(5 \times 2^7)^4 = 5^4 \times 2^{28}$
d'après (2) $5^4 \times 2^{28} \equiv -2^4 \times 2^{28} \equiv -2^{32} \pmod{641}$
Donc $-2^{32} \equiv 1 \pmod{641}$ ou encore $2^{32} + 1 \equiv 0 \pmod{641}$
Ce qui signifie que 641 divise $2^{32} + 1$.

II

Ex 1 :

Appel ons k le nombre tours de la première planète" autour de la terre", pour revenir à la verticale de A, et k ' celui de la deuxième planète. Il s'agit de déterminer k et k ' pour que :

$1 + 567\,k = 4 + 145\,k'$
ou encore : $567\,k - 145\,k' = 3$.

Ecrivons l'algorithme d'Euclide entre 567 et 145.

$567 = 3 \times 145 + 132$
$145 = 1 \times 132 + 13$
$132 = 10 \times 3 + 2$
$.13 = 6 \times 2 + 1$

567 et 145 sont premiers entre eux, et l'algorithme nous permet de savoir que

- $-67 \times 567 + 262 \times 145 = 1$
- donc $3(-67 \times 567 + 262 \times 145) = 3$.
- Ainsi nous avons trouvé un couple qui convient pour $(k ; k')$: $k_0 = -201$ et $k'_0 = -786$.

Nous avons donc : $567k_0 - 145k'_0 = 3$

Et $567k - 145k' \equiv 3$.

Nous en déduisons par différence que : $567(k - k_0) = 145(k' - k'_0)$.

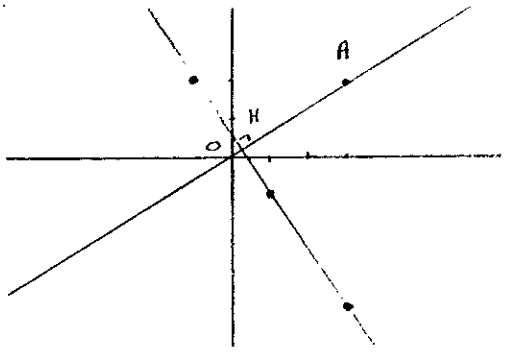
145 divise $(k - k_0)$ puisque 145 est premier avec 567 (Théorème de Gauss). Il existe donc un entier t tel que : $k - k_0 = 145t$ (et $k' - k'_0 = 567t$)
La plus petite valeur pour t, telle que k et k ' soient des entiers positifs est 2.
Nous trouvons alors que $k = 89$ et $k' = 348$.
Ce qui donne un nombre de jours à partir du 1° janvier 1999 de 50464 jours ($1 + 567 \times 89$), ou encore 138 années et 94 jours.

Ex 2 :

$au + bv = 1 \Leftrightarrow \overrightarrow{OM}.\overrightarrow{OA} = 1$.
Appelons H le projeté orthogonal de M sur (OA).
$au + bv = 1 \Leftrightarrow \overline{OH}.\overline{OA} = 1$.

Ainsi H est le point de (OA) tel que $OH = \frac{1}{OA}$ et $\overrightarrow{OH}$ et $\overrightarrow{OA}$ sont de même sens.

Les couples (u ; v) recherchés sont les coordonnées des points M de la droite perpendiculaire en H à (OA), points de coordonnées entières.



Ex 3 :

a et b sont premiers entre eux donc il existe un couple d'entiers (u ; v) tel que au + bv = 1.
Donc auc + bvc = c.
Si a divise bc, alors a divise auc et bvc, donc il divise c.

Question 1:

Soit a un nombre non premier. a possède donc un diviseur b tel que a = bq, avec $1 < b < a$.
Si b est premier, le théorème est démontré.
Si b n'est pas premier, il admet un diviseur c tel que b = cq ' avec $1 < c < b$.
Si c est premier c est aussi un diviseur de a, donc le théorème est démontré. Sinon, on recommence le raisonnement et on obtiendra une suite de nombres entiers décroissants minorés par 1. Cette suite est obligatoirement finie; le processus doit s'arrêter et dans cette suite il y aura donc un diviseur premier.

Ex 4 :

1° $304 = 2^4 \times 19$ $\quad 2880 = 2^6 \times 3^2 \times 5$ $\quad 864 = 2^5 \times 3^3$

Le PGCD des trois nombres est donc : 2^4 soit 16, et le PPCM est $2^6 \times 19 \times 3^3 \times 5 = 164160$.

2° La grandeur des nombres montre bien que la décomposition en produit de facteurs premiers risque d'être longue.
En fait $1100005423 = 11 \times 100000493$ et $1100000077 = 11 \times 100000007$

Et il n'est pas facile de montrer que 100000493 et 100000007 sont premiers entre eux.

Question 3:

Pour Gauss, les lettres a, b et c ...désignent encore des nombres positifs.

Ex 5 :

En continuant, nous écrirons que $3 = 1 \times 2 + 1$ donc $\frac{3}{2} = 1 + \frac{1}{2}$.

Alors reconstituant le tout nous aurons : $\frac{43}{35} = 1 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{2}}}}$

Donc $\frac{35}{43} = \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2 + \frac{1}{2}}}}$

Et en négligeant le dernier $\frac{1}{2}$ on obtient :

$$\cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2+1}}} = \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{3}}} = \cfrac{1}{1 + \frac{1}{\frac{13}{3}}} = \cfrac{1}{1 + \frac{3}{13}} = \frac{1}{\frac{16}{13}} = \frac{13}{16}$$

Or : $43 \times 13 = 559$ et $35 \times 16 = 560$. Donc $43 \times 13 = 35 \times 16 - 1$.

Ex 6 : $7u + 4v = 1$ a pour solution particulière $(u_0 ; v_0) = (-1 ; 2)$

$7u + 4v = 100$ a donc pour solution particulière $(-100 ; 200)$. Par suite les solutions de l'équation sont de la forme $u = -100 + 4k$ et $v = 200 - 7k$ où $k \in Z$; or $u > 0 \Leftrightarrow k > 25$ et $v > 0 \Leftrightarrow k \leq 28$. Il y a donc trois solutions possibles :

Si $k = 27$ alors $x = 8$, $y = 11$, et $z = 81$

Si $k = 28$ alors $x = 12$, $y = 4$, et $z = 84$.

Ex 7 : Soit n le nombre de pièces d'or. Les différentes hypothèses de partage se traduisent par le système :

$$\begin{cases} n = 17q_1 + 3 \\ n = 11q_2 + 4 \\ n = 6q_3 + 5 \end{cases}$$

On résout successivement les équations :

$17q_1 - 11q_2 = 1$ qui a pour solution $q_1 = 2 + 11k$ et $q_2 = 3 + 17k$

$11q_2 - 6q_3 = 1$ qui a pour solution $q_2 = -1 + 6k'$ et $q_3 = -2 + 11k'$

et enfin $3 + 17k = -1 + 6k'$ qui équivaut à $17k - 6k' = -4$ et qui a pour solution $k = 4 + 6p$ et $k' = 12 + 17p$.

On obtient alors $q_1 = 2 + 11(4 + 6p) = 46 + 66p$ et donc $n = 785 + 1122p$.

Le butin compte donc, au minimum, 785 pièces d'or.

Ex 8 : Soit n le nombre de majorettes prêtes à marcher au pas. Les différentes configurations conduisent au système :

$$\begin{cases} n = 4q_1 + 1 \\ n = 5q_2 + 2 \\ n = 7q_3 + 3 \end{cases}$$

De même qu'à l'exercice précédent, on résout successivement les équations :
$4q_1 - 5q_2 = 1$ qui a pour solution $q_1 = -1 + 5k$ et $q_2 = -1 + 4k$
$5q_2 - 7q_3 = 1$ qui a pour solution $q_2 = 3 + 7k'$ et $q_3 = 2 + 5k'$
et enfin $4k - 7k' = 4$ qui a pour solution $k = 8 + 7p$ et $k' = 4 + 4p$.
on revient au système initial et on obtient $n = 157 + 140p$ où p est un entier relatif. Comme on sait que $20 \leq n \leq 180$ alors $p = 0$; donc $n = 157$ et il y a $180 - 157 = 23$ majorettes qui sont restées à la maison.

Chapitre 4

Ex 1 : Puisque la constante est égale à 21, il suffit de réécrire l'alphabet en décalant de 21 places. Ainsi la lettre A (n° 1) a-t-elle été remplacée par la lettre n° 22, c'est-à-dire V :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Et maintenant il n'y a plus qu'à lire : GZN se lit LES ; MVXDIZN se lit RACINES, etc ...

Ex 2 :
NUL NE SAIT CE QU'EST UNE VARIABLE sera codé :
VQP VU KIGN OU EQ UKN QVU TIHGILPU

Ex 3 : Il s'agit du début d'un célèbre roman de Lewis Caroll qui commence par "Alice ..."

Ex 4 : ici $n = 33$, $c = 3$, $m = 20$ (car $33 = 3 \times 11$). On cherche alors d tel que $3d \equiv 1 \pmod{20}$; on trouve $d = 7$. On calcule 5^7 et $23^7 \pmod{33}$ et on trouve 14 23, ce qui se traduit par A4♦B3.

Eléments de corrigés pour le texte de Pascal

Constitution de la deuxième ligne de nombres :

$10 = n\,A + B \quad 10 \equiv B \pmod{A}$

$10^2 \equiv 10B \equiv C \pmod{A}$ etc...

Critère de divisibilité :

Le nombre $TVNM = M + 10N + 10^2V + 10^3T \equiv M + BN + CV + DT$

Donc TVNM est divisible par A si et seulement si $M + BN + CV + DT$ est divisible par A.

L'utilisation des congruences permet de simplifier la démonstration du critère de divisibilité énoncé par Pascal.

Biographies :

EUCLIDE d'Alexandrie ($IV^{ème}$-$V^{ème}$ av.J.C).On sait peu de choses sur la vie d'Euclide : la date et le lieu de sa naissance nous sont inconnus. Euclide a probablement reçu sa formation mathématique à Athènes ; il se serait installé à Alexandrie à l'époque où Ptolémée 1^{er} en fait le centre culturel du monde hellénistique. Euclide a écrit de nombreux ouvrages – au moins une dizaine – dont certains ont été perdus, mais son œuvre majeure est les *Eléments* qui comporte treize livres regroupant la plus grande partie des connaissances mathématiques du monde grec. Ce traité monumental a été, pendant deux millénaires, l'ouvrage le plus utilisé et étudié, après la Bible.

EULER Leonhard (1707-1783) est né à Bâle. Son père, pasteur calviniste d'un village voisin mais ancien élève de Jacques Bernoulli, l'initia aux mathématiques. Entré à l'Université de Bâle pour y étudier la théologie, Euler attira l'attention de Jean Bernoulli par ses aptitudes en mathématiques et devint l'ami de ses fils Nicolas, Daniel et Jean. Ceux-ci, établis à l'Académie de Saint-Pétersbourg le firent venir en Russie. Euler resta à Saint-Pétersbourg de 1727 à1741 puis se rendit à l'Académie de Berlin sur l'invitation du roi de Prusse où il resta jusqu'en 1766, date à laquelle Catherine II de Russie l'invita à revenir à Saint-Pétersbourg où il resta jusqu'à sa mort. Euler était doué d'une mémoire phénoménale, d'une intelligence aiguë et universelle et, bien qu'il fût devenu pratiquement aveugle en 1767, il continua de travailler jusqu'à sa mort. Il fut un mathématicien particulièrement fécond dans toutes les branches des mathématiques : théorie des nombres, analyse, nombres complexes, trigonométrie, équations différentielles, géométrie analytique et différentielle des courbes et des surfaces. C'est à lui que l'on doit l'usage des symboles e, π et i, la notation fonctionnelle fx, le symbole $\sum$ pour indiquer la sommation.

FERMAT Pierre de (1601-1665) est né à Beaumont-de-Lomagne et mort à Castres. Fils d'un riche négociant en cuir, Pierre de Fermat fait des études de droit à Toulouse, puis Bordeaux et enfin Orléans. En 1631 il achète une charge de conseiller au Parlement de Toulouse. C'est un amateur en mathématiques, au sens élogieux du terme : il lit et annote les œuvres de Diophante traduites par Bachet de Méziriac (c'est dans la marge de son exemplaire qu'est énoncé son fameux théorème), il correspond avec le cercle de Mersenne, en particulier avec Blaise Pascal avec qui il établit les prémisses du calcul des probabilités. Fermat a été un précurseur dans de nombreux domaines : théorie des nombres, probabilités, calcul infinitésimal, géométrie analytique. Mais n'ayant pas ou peu publié, son œuvre a eu peu de retentissement à son époque.

GAUSS Karl Friedrich (1777-1855) est né à Göttingen dans un milieu modeste et peu instruit. Ses professeurs surent reconnaître son génie précoce et l'aidèrent à poursuivre ses études. Il resta fidèle à la ville de Göttingen où il étudia, fonda et dirigea l'Observatoire, devint le Doyen de la Faculté, et mourut. Gauss fut un mathématicien génial - on le surnomma le "Prince des mathématiciens" - mais solitaire ; il publia peu et la découverte en 1898 de son journal mathématique, fort bref puisqu'il ne compte que dix-neuf pages, permit d'établir la date et l'authenticité de certains résultats. Ses travaux en mathématiques portèrent sur la théorie des nombres, les statistiques, l'élaboration d'une géométrie non-euclidienne. A partir de 1807 il se consacra davantage à l'astronomie et à la physique, domaines où ses contributions sont également riches et variées.

MERSENNE Marin (1588-1648) est né à Oizé, dans la Sarthe, et mort à l aris. Ce moine de l'ordre des Minimes était un érudit qui a entretenu une correspondance avec les plus grands savants de son époque : Descartes, Pascal, Torricelli, Gassendi, Hobbes, Huygens, Roberval, etc... En plus d'enseigner la philosophie, de mettre au point un télescope à miroir parabolique, de mesurer la vitesse du son, il s'intéresse aux mathématiques, en particulier à la primalité

des nombres de la forme $2^n - 1$, connus d'Euclide, mais qui portent son nom depuis le XVII^{ème}siècle.

PASCAL Blaise (1623-1662) est né à Clermont-Ferrand et mort à Paris. Ayant perdu sa mère à l'âge de trois ans, il est élevé par son père juriste passionné de mathématiques, qui s'installe à Paris en 1631 et se consacre à l'éducation de son fils. Il le fait participer aux réunions organisées chez Mersenne et le jeune Blaise Pascal s'intéresse à la géométrie : il écrit, à seize ans, un *Essay pour les coniques* qui impressionne Descartes. En 1654, Blaise Pascal est frappé par une extase religieuse et entre au couvent janséniste de Port-Royal ; il se détourne alors des sciences qu'il juge incompatibles avec son engagement religieux. C'est à cette époque qu'il écrit *Les Pensées* et *Les Provinciales.* A partir de 1658 il revient cependant aux mathématiques : géométrie mais aussi probabilités et analyse infinitésimale où ses travaux, faisant suite à ceux de Stévin, Roberval et Descartes, inspireront ceux de Newton et Leibniz.

Bibliographie

Chabert, J-L., et alii, *Histoire d'algorithmes*, Belin, Regards sur la science, 1994

Collette, J-P., 2 volumes, Vuibert, 1973-1979

Conway, J. et Guy, R., *Le livre des nombres*, Eyrolles, 1998

Delahaye J-P., *Merveilleux nombres premiers*, Belin, Pour la Science, 2000

Duffaud, B., et alii, *Arithmétique en Terminale S*, Besançon, IREM, 1998

Euclide, *Œuvres*, trad. F.Peyrard, Patris, Paris,1819, Réed. Blanchard, Paris, 1966

Fitz-Patrick, J., *Exercices d'arithmétique*, 1914, Réed. Gabay, 1995

Galois, E., *Ecrits et mémoires mathématiques*, Réed. Gabay, 1997

Groupe de travail sur la liaison Lycée-Université, *Cours et activités en arithmétique pour les classes terminales*, Marseille, IREM, 1998

Guedj, D., *L'empire des nombres*, Gallimard, Découvertes, 1996

Guinot, M., *Arithmétique pour amateurs : Pythagore, Euclide et toute la clique,* Aleas, 1992

Guinot, M., *Ce diable d'homme d'Euler,* Aleas 1995

Guinot, M., *Gauss, le prince des mathématiciens,* Aleas 1997

Guinot, M., *Les resveries de Fermat,* Aleas, 1994

Guinot, M., *Une époque de transition : Lagrange et Legendre,* Aleas 1996

Kendall, P.M.H. and Thomas, G.M., *Mathematical Puzzles for the connoisseur*, Griffin, 1962

Le Lionnais, F., *Les nombres remarquables*, Hermann, 1983

Mendès-France, M. et Tenenbaum, G., *Les nombres premiers*, PUF, QUE sais-je ? n° 571, 1997

Molk J. (sous la direction de), *Encyclopédie des Sciences Mathématiques pures et appliquées*, Tome 1, 3ème volume Théorie des nombres, Paris, Gauthier-Villars, 1904-1916, Réed. Gabay, 1991

Rashed,R., *Entre arithmétique et algèbre*, Les belles lettres, 1984

Robin, G., *Apprenons l'arithmétique élémentaire pour comprendre la cryptographie moderne*, Limoges, IREM, 1998

Sierpinsky,W., *Problèmes de théorie élémentaire des nombres*, 1970, Gabay, 1992

Singh, S., *Histoire des codes secrets*, J-C.Lattès, 1999

Singh, S., *Le dernier théorème de Fermat*, J.C.Lattès, 1998

Trignant, J., *Fractions continues*, Editions du choix, 1994

Warusfel, A., *Les nombres et leurs mystères*, Seuil, Points Sciences S21, 1961

Wells, D., *Le dictionnaire Penguin des nombres curieux*, Eyrolles, 1995

Revues :

La Recherche, numéro spécial « Nombres » , Juillet-Août 1995

Les cahiers de Science et vie n° 57, Juin 2000

Tangente, Hors-série n° 6 « Secrets de nombres », 1999

Sites internet :

http://titan.glo.be/tsf/index.html (sur la cryptographie)

http://www.multimania.com/marief/ (sur la cryptographie)

www.utm.edu/research/primes (sur les nombres premiers)

http://chronomath.irem.univ-mrs.fr/ (sur l'histoire des mathématiques)

Table des matières