LES NOUVEAUX PROGRAMMES DE TERMINALE S
ARITHMÉTIQUE

Cet exposé s'inspire largement, entre autres, de comptes-rendus de réunions d'Inspecteurs Généraux et d'Inspecteurs Pédagogiques Régionaux, ainsi que d'un atelier du colloque interacadémique de Toulouse sur ce sujet (printemps 98).

Mais il vise principalement à donner des matériaux pour l'enseignement et surtout pour la réflexion, dont certains sont personnels à l'animateur ; l'ensemble de cet exposé n'engage donc que celui-ci : C. Drouin, professeur au Lycée de Pauillac (Gironde).

PLAN

Après avoir parlé de la structure même du cours d'arithmétique, nous réfléchirons sur quelques points particuliers : algorithmes et programmation, congruences…

1. Organisation générale de l'enseignement de l'arithmétique

1.1. Idées directrices

D'après diverses réunions de réflexions sur les nouveaux programmes :

Il est conseillé de répartir l'enseignement de l'Arithmétique sur 20 à 25 heures, réparties en deux ou trois périodes.

Les connaissances et savoir-faire exigibles sont modestes, afin de laisser du temps aux travaux pratiques et aux activités, qui visent à la formation de l'esprit scientifique, et à la préparation à l'enseignement supérieur, et afin d'éviter, autant que possible, le bachotage.

On fera bien la différence entre les concepts traités en cours conformément au programme, et les problèmes ou applications traités à titre d'exemples et d'activités. Rentrent entre autres dans la deuxième catégorie : la relation « ab = dm », le corollaire immédiat du théorème de Gauss, la formule donnant le nombre de diviseurs d'un entier…Aucune connaissance spécifique ne peut être exigée des élèves sur la notion de congruence, par exemple au baccalauréat.

On souligne que les programmes accordent une grande importance aux **aspects algorithmiques** des concepts de l'arithmétique.

Il faut donc bien noter que parmi les activités et exercices proposés dans la suite de l'exposé, les plus difficiles sont clairement de l'ordre de la proposition, et non de la norme ! (Ne serait-ce que par manque de temps) De plus certains textes visent plus à amorcer une réflexion de la part de l'enseignant qu'à être directement posés en classe.

Esprit général du programme

« Il s'agit de trouver un équilibre entre le rôle de la décomposition en produit de facteurs premiers et celui de la division euclidienne. Il est ainsi conseillé de donner son plein rôle à la division euclidienne, et de limiter le recours à la décomposition en produit de facteurs premiers ».

1.2. Propriétés fondamentales de **N**.

En accord avec les groupes de travail, il convient de mettre clairement en évidence les propriétés fondamentales de **N** (et donc de **Z**).

En particulier faire le lien entre ces diverses propriétés de **N**, toutes équivalentes entre elles :

Principe" de récurrence

Toute partie non vide de N admet un plus petit élément.

Toute suite décroissante d'entiers finit par être constante.

Cependant, il n'est pas question de construire **N** et **Z** par les axiomes de Peano. Les propriétés algébriques de ces deux ensembles sont admises. Dans ce cas, c'est sans doute la propriété **du plus petit élément** de la partie non vide qui est la plus commode à mettre à la base. L'axiome de récurrence devient alors un théorème.

Remarquons que la notion de **partie entière** d'un rationnel est liée à cette propriété fondamentale de **N**, ou, ce qui revient au même, à la division euclidienne dans **Z**.

1.3. Notions principales ; grands théorèmes ; exercices classiques.

Dans le désordre :

Divisibilité ; PGDC, PPMC ; nombres premiers entre eux ; nombres premiers ;
division Euclidienne ; théorème de Gauss ;
algorithme d'Euclide pour le PGDC ; théorème de Bezout
$D_a \cap D_b = D_d$ avec d = PGDC(a,b).
Unicité de la décomposition en produit de facteurs premiers (admis)
Expression du PPMC et PGDC en produit de facteurs premiers.
Algorithmes.
pas explicitement au programme : " a**Z** + b**Z** = d**Z"** dm = ∣ ab ∣

Remarques du groupe de travail

• La division euclidienne à traiter est celle d'un entier relatif par un entier naturel non nul, voire celle d'un entier naturel par un autre (non nul). Il ne semble pas très utile de traiter la division euclidienne par un entier relatif non nul.

• On ne traite que des PGDC, PPMC de DEUX entiers relatifs.

• Le corollaire du théorème de Gauss : « Si p et q sont premiers entre eux, si p divise n et q divise n, alors pq divise n » n'est pas explicitement au programme. Il ne peut donc normalement pas être *supposé connu* dans la résolution d'un exercice de baccalauréat (il est cependant intéressant).

Idem pour le théorème : « Si p est premier avec n et q premier avec n, alors pq est premier avec n ».

Grands TP et exercices :

Ensemble des diviseurs

Base de numération

Critère de divisibilité

Résolution de ax + by = c

Calendriers

Codages

Congruences (facultatif)

Pas explicitement au programme mais classiques :

Petit théorème de Fermat

Théorème de Wilson

Nombres parfaits, de Mersenne, de Fermat…

1.3. Moyens principaux de démonstration

Quels sont les outils principaux ? Ce sont :
- La division euclidienne.
- L'algorithme d'Euclide.
- La propriété du plus petit élément. (ou le principe de récurrence)
- Éventuellement, des résultats qui sont des résultats sur les idéaux, sans bien sûr utiliser le vocabulaire des idéaux.

À propos du théorème de Bezout :

Remarquons que **l'algorithme d'Euclide** fournit une démonstration du théorème de Bezout. [Soient a et b deux entiers naturels et d leur PGDC. Il existe des entiers relatifs u et v tels que au + bv = d.]

(On peut aussi utiliser la démonstration reposant sur le fait que a**Z** + b**Z** est un idéal de **Z**, donc de la forme x**Z,** avec x ∣ d et d ∣ x (sans utiliser, bien sûr, ce vocabulaire avec les élèves !)

1.4. Les progressions possibles

Il y a deux progressions principales : L'une commençant par la décomposition en produit de facteurs premiers ; l'autre par la division euclidienne, PGDC, PPMC…

La **première progression**, dans laquelle on commence par la *décomposition en produit de facteurs premiers* (théorème fondamental de l'Arithmétique), paraît la plus naturelle à la lecture des programmes.

Il y a cependant deux difficultés :

• La première difficulté est que la **démonstration de l'unicité de la décomposition de tout entier naturel en produit de facteurs premiers, est hors programme.**

Cependant le "Terracher" (en exercice) ou l'ouvrage à paraître de l'IREM de Bordeaux proposent une démonstration. Seul le second ouvrage enchaîne en démontrant : $D_a \cap D_b = D_d$, ainsi que le théorème de Gauss, utilisant ainsi à plein l'outil "décomposition en produit de nombres premiers".

• Deuxième difficulté : **Part peut-être trop belle faite à un type de raisonnement peu essentiel, au détriment de la division euclidienne ou d'autres méthodes**, en contradiction avec les conseils rapportés au § B.2.

La **seconde progression** met le *Théorème de Gauss avant le théorème de décomposition en produits de facteurs premiers*. C'est elle qui a eu la préférence des divers ateliers de réflexion.

Remarquons que si l'on dispose du théorème de Gauss, il me semble très aisé de démontrer l'unicité de la décomposition primaire.

D'où vient alors le théorème de Gauss ? la progression la plus naturelle semble être la suivante :

Division Euclidienne > PGDC > Algorithme d'Euclide > $Da \cap Db = Dd$ > Théorème de Gauss.

Je propose en Annexe 1 :

– Une démonstration du Théorème de Gauss par récurrence, qui n'utilise ni les nombres premiers, ni l'algorithme d'Euclide ni le théorème : « $D_a \cap D_b = D_d$ ». Cette démonstration permet d'envisager un autre type de progression, où la division euclidienne et l'algorithme d'Euclide, ainsi que l'unicité de la décomposition primaire viendraient **après** le Théorème de Gauss.

– Également, une démonstration de l'unicité de la décomposition en produit de facteurs premiers n'utilisant pas le théorème de Gauss. Cette démonstration se situe dans le cadre de la première progression ci-dessus et se propose comme alternative à celle qui figure dans le "Terracher" ou l'ouvrage de l'IREM de Bordeaux.

Deux exemples de progression

Progression 1	**Progression 2**
1. Divisibilité et division euclidienne dans **Z** – Diviseurs – Division euclidienne TP: Notion de congruence ; compatibilité avec l'addition et la multiplication. Exemples de critères de divisibilité. Exemples de changements de base de numération. Exemples de calendriers.	
2. Diviseurs communs à deux entiers. # PGCD # Algorithme d'Euclide # Théorème de Bezout # Théorème de Gauss TP : exemples de résolution d'une équation au + bv = d. Exemples de cryptages. 3. Multiples communs à deux entiers. # PPCM # Relation entre PPCM et PGCD 4. Nombres premiers # Définition # Existence d'une infinité de N.Pr. # Décomposition d'un entier en produit de facteurs premiers. TP : Crible d'Ératosthène Reconnaissance d'un nbre premier. Recherches de PPCM et PGCD Liste des diviseurs d'un entier.	2. Nombres premiers # Définition # Existence d'une infinité de N.Pr. # Décomposition d'un entier en produit de facteurs premiers. TP : Crible d'Ératosthène Reconnaissance d'un nbre premier. 3. Nombres premiers entre eux # Définition # Théorème de Bezout # Théorème de Gauss TP : Exemples de cryptages. 4. Décomposition en produits de facteurs premiers. TP : liste des diviseurs d'un entier. 5. Diviseurs et Multiples communs à deux entiers. # PGCD # Algorithme d'Euclide # PPMC # Relation entre PPCM et PGCD TP : Recherches de PPCM et PGCD Exemples de résolution de au + bv = d.

Une proposition personnelle de progression. **1. Multiples et diviseurs.** # Ensembles **N**, **Z**, **Q** ; récurrence. # Multiples, diviseurs, ppmc, pgdc # Théorème de Gauss **2. Division euclidienne + Alg. d'Euclide** # Division euclidienne # Algorithme d'Euclide ; # Bases de numération # Congruences	**3. Nombres premiers.** # Décomposition en nombres premiers ; son unicité. # Application au PPMC et au PGDC. **4. Nouveaux théorèmes sur le pgdc et ppmc**. # $aZ \cap bZ = mZ$; $md = ab$ # Égalité de Bezout ; équation au + bv = c.

Pour utiliser cette progression, on peut envisager de démontrer le théorème de Gauss par récurrence, comme suggéré plus haut et comme décrit en annexe.

2. Algorithmes

La difficulté est de tenir compte de la diversité des calculatrices et des logiciels.

L'essentiel ne réside certainement pas dans la programmation elle-même, mais dans la compréhension de l'algorithme.

On trouvera dans le manuel "Déclic" (Hachette) des programmes pour les calculatrices les plus courantes.

Le reste de la division euclidienne de a par b pourra être obtenu par : r = a – int(a/b)*b.

La proposition : a divise b pourra alors être obtenu par : r = 0.

Test de primalité :	Algorithme d'Euclide :
Demander n ; 2 – >p (p est le diviseur éventuel)	Demander a et b, avec a < b.
☺ (étiquette)	a – > m et b – > n
Si $p^2 \geq n$ alors	☺ (étiquette)
afficher : p est premier	Soit r le reste de la division euclidienne de n par m.
fin	Si r ≠ 0 alors :
Si p divise n alors :	m – > n , r – > m
afficher : "n n'est pas premier", ainsi que son diviseur p.	aller en ☺
Si p ne divise pas n, alors :	Si r = 0, alors :
p + 1 – > p	afficher m (qui est le PGDC)
aller en ☺	fin

Algorithme pour la congruence de a^x modulo n

Demander a , demander n, demander x, m = 1 (On va considérer les restes des a^m)

on affecte à r le reste de la division euclidienne de a par n.

r – > s (s est le reste modulo n de a^m)

☺ (étiquette)

Si m = x alors afficher s fin

Si m ≠ x alors :

m + 1 – > m

on affecte à s le reste de la division euclidienne de r.s par n.

aller en ☺

Il s'agit donc d'une exploitation de l'algorithme d'Euclide pour trouver les coefficients dans l'égalité de Bezout. L'algorithme est intéressant, car on l'applique tout aussi bien "à la main", mais de façon un peu différente. À chaque dernier nombre m donné par l'algorithme d'Euclide, u et v sont des variables telles que : **ua + vb = m**. Mais on a besoin aussi de l'étape précédente, à savoir : **sa + tb = n** Alors la troisième égalité, n – qm = r, qui provient de la division euclidienne, fournit : (s – qu)a + (t – qv)b = r. Il faut donc faire : m – > n , r – > m , u – > s , v – > t , s – qu – > u , t – qv – > v.	**Égalité de Bezout : algorithme** Demander a et b, avec a < b. a – > m et b – > n, 1 – > u , 0 – > v ; 0 – > s ; 1 – > t ☺ (étiquette) Soit r le reste de la division euclidienne de n par m et q le quotient Si r ≠ 0 alors : m – > n , r – > m , u – > s , v – > t , s - qu > u, t – qv – > v aller en ☺ Si r = 0 alors : afficher m (le pgdc : d) , afficher u et v (on a : au + bv = d)

On pourra en classe faire remarquer que la façon humaine de procéder diffère de la façon informatique. Ceci provient du fait qu'il ne nous coûte rien de mémoriser, sur le papier, les calculs intermédiaires. L'ordinateur pourrait aussi le faire, mais il faudrait alors un tableau (une liste).

Exemple : Partie mathématique Soit a = 11 et b = 26 $26 = 2 \times 11 + 4$ $-2 \times 11 + 26 = 4$ $11 = 2 \times 4 + 3$ d'où $11 - 2 \times 4 = 3$ d'où $5 \times 11 - 2 \times 26 = 3$ $4 = 3 + 1$ d'où $4 - 3 = 1$ d'où $-7 \times 11 + 3 \times 26 = 1$ $3 = 3 \times 1 + 0$ 1 est le pgdc de 11 et 26.	Partie informatique m = 11, n = 26, u = 1, v = 0, s = 0, t = 1 q = 2, r = 4 n = 11, m = 4, **u = – 2, v = 1**, s = 1, t = 0 q = 2, r = 3 n = 4, m = 3, **u = 5, v = – 2**, s = – 2, t = 1 q = 1, r = 1 n = 3, m = 1, **u = – 7, v = 3**, s = 5, v = – 2 r = 0, on arrête tout on affiche : **d = m = 1, u = – 7, v = 3**,

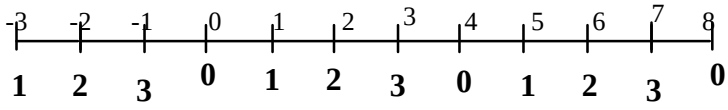
3. Sur la congruence

Programme Sur des exemples, utilisation de la division euclidienne pour établir des critères de divisibilité. Exemples de changements de base de numération.	La division euclidienne permet d'établir des compatibilités avec les opérations nécessaires pour les problèmes étudiés. Ceux-ci pourront être l'occasion de présenter et de mettre en œuvre la notion de congruence, **au sujet de laquelle aucune connaissance spécifique ne peut être exigée.** Toute introduction de **Z**/n**Z** est hors programme. l'aspect algorithmique sera privilégié.

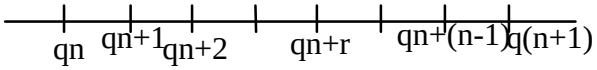
D'autre part, d'après le groupe de travail disciplinaire :

" ***Les congruences sont à comprendre comme une exploitation du fait que l'ensemble des entiers naturels est union de sous-ensembles (les classes). Une représentation géométrique des entiers sur un axe, distingués suivant la nature de leur reste dans la division euclidienne par un entier donné est conseillée."***

Voici par exemple une représentation des entiers suivant leur reste dans la division euclidienne par 4 (c'est-à-dire : modulo 4).



Cette représentation géométrique peut faire suite à celle de la division euclidienne (cf. par exemple le Transmath)



• Il est opportun de dresser des tables d'addition ou de multiplication de Z/nZ dans quelques cas particuliers pour des activités d'études de lignes, de colonnes… par exemple, dans la table de multiplication de Z/6Z, étudier la ligne des multiples de la classe 4 : valeurs atteintes, produits trouvés plusieurs fois, valeurs non atteintes. Même étude pour les multiples de la classe 5. dans la table de multiplication de la classe 7, étudier les mêmes questions

Voir en ANNEXE 2 un essai d'application.

Exercices amenant à utiliser les congruences (ou du moins les restes)

Exercice : *Montrer que $a^2 + b^2$ est divisible par 3 ssi a et b le sont*.

La seule solution, me semble-t-il, consiste à considérer les restes des divisions euclidiennes de a et b par 3, et à expliciter le tableau suivant.

reste dans la division par 3 de a>		0	1	2
	de a^2 >	0	1	1
de b	de b^2	de $a^2 + b^2$		
0	0	0	1	1
1	1	1	2	1
2	1	1	2	1

Exercice : *Étudier, selon les valeurs de l'entier naturel n, le reste de la division euclidienne de 7^n par 10.*

La méthode naturelle, me semble-t-il, est d'utiliser les congruences, ou du moins les restes dans la division euclidienne par 10 des puissances successives de 7.

puissances successives de 7	7^1	7^2	7^3	7^4	7^5	7^6 …
reste dans la division par 10	7	9	3	**1**	7	9…

Ce tableau amène à penser que le reste modulo 10 de 7^n ne dépend que du reste de n dans la division euclidienne par 4. (on voit ainsi apparaître un nouveau diviseur de division euclidienne.) Cette conjecture peut être aisément démontrée.

En effet, $7^{4q + s} = 7^{4q} \times 7^s$. Or $7^{4q} = (7^4)^q$. Ce dernier nombre a donc même reste dans la division par 10 que $1^q = 1$. Donc, grâce à la compatibilité avec la multiplication, $7^{4q + s} = 7^{4q} \times 7^s$ a même reste dans la division par q que 1×7^s , soit 7^s.

Ceci permet de répondre à la question posée, à partir du reste de n dans la division euclidienne par 4.

Exercices : Reste de la division par 5 du carré d'un entier ; de la puissance quatrième d'un entier. Reste de la division par 7 du carré d'un entier ; du cube d'une entier ; de la puissance quatrième d'un entier.

Exercice :Démontrer que si $n = p^2 + 2$ est premier, alors p est divisible par 9.

Indication : On s'intéressera au reste de n dans la division par 3.

Exercice : Existe-t-il des entiers naturels n tels que $2^n + 3^n$ soit divisible par 7 ?

Exercice :

a. Étudier, selon les valeurs de l'entier naturel n, le reste de la division euclidienne de 7^n par 10.

b. Déterminer, suivant les valeurs de n, le chiffre des unités de $A = 1 + 7 + 7^2 + \ldots + 7^n$.

Exercice : Chercher le reste de la division euclidienne de 37^{28} par 7.

Exercice : Chercher le reste de la division euclidienne de 4^{1998} par 7.

Exercice : Quels sont les entiers n tels que $2^n - 1$ soit divisible par 9 ? Cette condition étant vérifiée, montrer que $2^n - 1$ est divisible par 63.

Exercice : Paraît vraiment difficile au niveau Terminale : Démontrer que pour tout entier naturel non nul n, $n^7 - n$ est divisible par 42.

Dans un autre style, avec une pertinence à discuter :

Exercice : trouver les nombres entiers qui soient à la fois congrus à 1 modulo 3 et congrus à 2 modulo 7.

4. Activités classiques

Remarque préliminaire ; " classique" ne veut en aucun cas dire nécessaire ou obligatoire.

4.1. Les codages

En préliminaire au *codage* , on peut dire un mot du *chiffrage* ou numérisation. En effet, le codage proprement dit va transformer un nombre en un autre nombre. Il s'agit donc d'abord de convertit une lettre ou un caractère (par exemple un espace), en nombre. On peut par exemple associer à toute lettre sa place dans l'alphabet, de 01 à 25, ou utiliser le code ASCII.

Mais il faut à une certaine étape briser la bijection lettre/nombre car celle-ci permettrait à un intrus par une étude des fréquences des lettres, de traduire les nombres les plus souvent répétés en lettres, et donc de commencer à décoder le message. Pour empêcher cela, on peut par exemple, après avoir écrit les nombres de 01 à 26 représentant les lettres, regrouper les chiffres par tranches de trois. Ainsi SALUTS = 19 01 12 21 20 19 deviendrait 190 112 120 019 , et ce seraient les nombres de trois chiffres qui seraient codés… Cependant, comme c'est dans cet exposé l'aspect mathématique qui nous intéresse, nous coderons de façon naïve les lettres une par une, par les nombres de 1 à 26.

Il me semble que le manuel " Hachette Éducation" (Terracher) présente diverses formes intéressantes de codages. Nous supposerons ici que nous raisonnons toujours modulo 27.

On peut considérer

– des codages **additifs** (à un nombre x on associe le reste de x + a modulo 27),

– des codages **multiplicatifs** (à x on associe le reste de a.x) qui sont mathématiquement intéressants, car leur décodage débouche sur l'égalité de Bezout ;

– des codages **affines**.

Voir aussi un codage dans $(\mathbf{Z}/27\mathbf{Z})\times$ $(\mathbf{Z}/27\mathbf{Z})$ dans le " Terracher" ;

– des codages **par fonction puissance :** à x on associe le reste de x^a modulo p. Il est sans doute plus intéressant de prendre alors : p premier, par exemple p = 29. Le décodage de ce code est alors lié au **petit théorème de Fermat** et à l'égalité de Bezout.

Remarque : À partir des codages de type " puissance" , les théorèmes utilisés sont plus compliqués et les exercices plus difficiles. Une activité par exemple sur le codage RSA paraît assez lourde à mettre en œuvre. Le travail pourrait peut-être, avec une classe dynamique, être proposé largement en devoir à la maison.

Voir en annexe 3 un présentation, qui a essayé d'être élémentaire, du codage RSA.

4.2. Le petit théorème de FERMAT

Théorème : Soit p un nombre premier et n un entier relatif. Alors p divise $n^p - n$. De plus, si n n'est pas divisible par p, p divise p divise $n^{(p-1)} - 1$.

Première démonstration : La première partie est démontrée par récurrence sur n, à partir de la formule du binôme et du fait que p divise tous les coefficients binomiaux C_p^k.

Autre démonstration : Une autre démonstration du petit théorème de Fermat est donnée par exemple par le Nathan Transmath.

On montre d'abord la deuxième partie de l'énoncé, en considérant, pour un entier relatif n non divisible par p, l'ensemble $\{r_1, r_2, \ldots r_{(p-1)}\}$ des restes respectifs des divisions euclidiennes de : 1n, 2n, …, (p – 1)n par p. Ces restes sont tous distincts, donc égaux, dans leur ensemble, à {1, 2, …(p – 1)}.

Par compatibilité avec la multiplication, les produits A = 1n.2n . …. (p – 1)n et $B = r_1.r_2. \ldots r_{(p-1)} = 1.2.3. .(p-1)$ ont alors même reste modulo p. On en déduit que p divise $n^{(p-1)} - 1$.

La première partie du théorème en découle.

4.3. Quelques nombres remarquables

Les deux derniers chapitres de "Histoire des mathématiques, Histoire de Problèmes", InterIREM, Ellipses, m'ont paru très intéressants sur ces sujets.

Nombres parfaits

Un nombre parfait est un nombre égal à la somme de ses diviseurs stricts (càd : qui lui sont strictement inférieurs). Le résultat mathématique est que tout nombre parfait pair est de la forme $2^n(2^{n+1}-1)$, mais on ne sait toujours pas s'il existe des nombres parfaits impairs. On peut faire démontrer par les élèves que si n est un nombre parfait de la forme $2^n p$, $n \geq 1$, avec p nombre premier, alors p est impérativement de la forme :

$p = 2^{n+1} - 1$.(Voir par exemple Nathan 99, page 129). Il est plus difficile de démontrer que tout nombre parfait pair est de la forme $2^n p$, $n \geq 1$, avec p nombre premier.

La preuve d'Euler procède ainsi. (Voir : Histoire des maths, histoire des problèmes, dernier chapitre)

Soit $N = 2^n p$, $n \geq 1$, avec p impair, un nombre parfait. Notons $\sigma(k)$ la somme des diviseurs positifs de tout entier k. On a alors :$\sigma(N) = 2N$. On peut montrer : $\sigma(N) = \sigma(2^n p) = \sigma(2^n) \cdot \sigma(p)$.

On en déduit: $2^{(n+1)}p = (2^{n+1} - 1)\sigma(p)$. (*) Alors $(2^{n+1} - 1)$ divise p : $p = k(2^{n+1} - 1)$.

L'égalité (*) fournit : $2^{n+1}.p = \sigma(p)$. D'où : $p + k = \sigma(p)$ (**).

On en déduit k = 1. Donc : $p = 2^{n+1} - 1$. Mais d'après (**), p est premier. CQFD.

Il y a des formules analogues, mais compliquées, qui donnent des nombres amiables ou amicaux : tels que la somme de tous les diviseurs propres de l'un soit égale à l'autre nombre.

Nombres de Mersenne

On appelle nombre de Mersenne un nombre de la forme : $M_n = 2^n - 1$, où n est un entier naturel. On démontre aisément qu'une condition nécessaire (mais non suffisante) pour que M_n soit premier est que n soit premier. Pour des compléments : voit TP4, page 70, Fractale (Bordas), 6.3 page 151, Transmath (Nathan), Secrets de Nombre (tangente/Archimède): $M_{859\,433}$ est premier. Un nombre de Mersenne premier est appelé : "nombre d'Euclide".

Nombres de Fermat

On appelle un nombre de Fermat un nombre de la forme : $F_j = 2^{2^j} + 1$, où j est un entier naturel. Posons : $N_n = 2^n + 1$.

• Nous nous proposons de montrer que les seuls nombres N_n premiers, sont les nombres de Fermat. Pour cela, nous allons démontrer que si N_n n'est pas un nombre de Fermat, alors N_n n'est pas premier.

- Démontrer que si N_n n'est pas un nombre de Fermat, alors n admet un diviseur impair p.

- En déduire que N_n n'est pas premier. [On pourra utiliser l'égalité : $x^p + 1 = (x + 1)(\ldots$].

• F_5 n'est pas premier.

• Soient F_i et F_j deux nombres de Fermat avec $i \neq j$.

Démontrer qu'il existe un nombre p pair tel que $F_i - 1 = (F_j - 1)^p$.

En déduire une égalité de la forme $aF_i + bF_j = 2$.

Quels sont alors les PGDC possibles de F_i et F_j ?

Démontrer que F_i et F_j sont premiers entre eux.

4.4 . Nombre de FAREY ; Approximation rationnelle d'un rationnel.

Définition: On dira que **deux fractions irréductibles m/n et m'/n' sont *"consécutives"*** si $m/n < m'/n'$ et s'il n'existe pas de fraction a/b comprise dans l'intervalle ouvert $]m/n, m'/n'[$ et telle que b soit inférieure au plus petit des deux dénominateurs n et n'.

Résultat : **Deux fractions irréductibles m/n et m'/n' sont consécutives si et seulement si on a : nm' – mn' = 1 (*)**

Démonstration :

- Démontrer d'abord que si la relation (*) est vérifiée , alors les deux fractions sont effectivement consécutives (comparer a/b – m/n et m'/n' – m/n, dans le cas où b est inférieur à min(n,n')).
- Inversement, soit m/n et m'/n' deux fractions irréductibles ne vérifiant pas la condition(*). On suppose d'abord : $n \leq n'$. Démontrer que l'équation nx – my = 1 a des solutions en entiers, puis donner tous les couples d'entiers solutions à partir d'une solution (x_0, y_0). Démontrer qu'un des couples (m", n") solution est tel que $1 \leq n" < n$. Conclure d'après la démonstration du sens direct que les fractions m/n et m'/n' ne sont pas consécutives. Procéder de façon similaire dans le cas n'<n, en considérant l'équation : xm' – yn' = 1.

Définition : Soit N un entier naturel non-nul. On appelle " suite de Farey" d'ordre N la suite finie des fractions irréductibles inférieures ou égales à 1, dont le dénominateur vaut au plus N, classées dans l'ordre croissant.

Exemple : la suite de Farey d'ordre 7 est :

0/1, 1/7, 1/6 , 1/5 , 1/4 , 2/7, 1/3, 2/5 , 3/7, 1/2, 4/7, 3/5, 2/3, 5/7, 3/4, 4/5, 5/5, 6/7, 1/1.

Il est alors immédiat que deux termes successifs d'une suite de Farey : m/n et m'/n', sont consécutifs au sens ci-dessus. Donc, d'après le " Résultat" : nm' – mn' = 1.(proposition 1).

Examinons maintenant comment une nouvelle fraction s'insère dans la précédente suite de Farey. Supposons que m/n et m"/n" soient consécutifs dans une suite de Farey, et que dans une suite de Farey postérieure on ait comme termes consécutifs : m/n, m'/n', m"/n". (m', n') est une solution de nx – my = 1. (m",n") est la solution suivante, donc :

m" = m + m', n" = n + n' (proposition 2).

Telle est la formule qui donne l'insertion d'une nouvelle fraction. Il faut donc rechercher les dénominateurs de fractions consécutives dont la somme est égale au nouvel ordre de Farey.

Par exemple, avant la suite de Farey d'ordre 7 ci-dessus, nous avions celle d'ordre 5: 0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/5, 1/1**.**

Les fractions consécutives dont la somme des dénominateurs fait 7 sont (1/4, 1/3), entre lesquels va s'intercaler 2/7, (2/5, 1/2), qui va donner naissance à 3/7 etc.

On peut aussi montrer, plus généralement :

Proposition 3. : Si m/n, m'/n', m"/n" sont trois termes successifs d'une suite de Farey, alors m'/n' = (m + m") / (n + n").

Farey était un géologue britannique. Il introduisit en 1816 les suites qui portent son nom, en en énonçant les propriétés que nous venons de voir. Cauchy compléta ses preuves.

On peut aussi parler de l'approximation rationnelle d'un réel, par exemple sous l'aspect graphique, pour commencer. Les meilleures fractions approximantes sont les réduites de la fraction continuée. Le " Résultat" ci-dessus permet d'affirmer que deux réduites consécutives m/n et m'/n' vérifient l'équation : nm' – mn' = 1 ou – 1.

4.5. Suite de FIBONACCI

(Condamine, manuel de Te.C, Algèbre, Delagrave, 1971)

Soit la suite définie par récurrence par : $u_0 = 1$, , $u_1 = 1$, et pour tout entier n supérieur ou égal à 2: $u_n = u_{n-1} + u_{n-2}$. Les relations suivantes sont intéressantes au point de vue arithmétique :

Pour tout entier naturel n supérieur ou égal à 2 : $u_{n+1}.u_{n-1} - u_n^2 = (-1)^2$.

Pour n et $p \geq 2$: $u_{n+.p} = u_n.u_{p-1} - u_{n-1}.u_p$.

On en déduit : **$PGDC(u_{n+p}, u_n) = PGDC(u_p, u_n)$**.

Alors, si r est le reste de la division euclidienne de m par n : **$PGDC(u_m, u_n) = PGDC(u_r, u_n)$.**

Et enfin : **$PGDC(u_m, u_n) = u_d$ avec : d = PGDC(m,n)**

5. Quelques exercices complémentaires

Divisibilité

Exercice : Trouver les entiers naturels n tels que la fraction $(n + 17) / (n - 4)$ soit un entier.

Exercice : Trouver les valeurs de l'entier p telles que p – 1 divise p + 11.

Exercice : Pour n entier relatif, on note $P(n) = n^2 + n + 1$.

- Trouver un petit entier naturel n tel que P(n) soit divisible par 13. (3 fonctionne)
- Caractériser tous les entiers naturels n tels que P(n) soit divisible par 13.

Exercice

On cherche tous les carrés d'entiers non nuls s'écrivant dans le système décimal : aabb.

- Démontrer alors que 100 a + b est le produit de 11 par un carré.
- Déterminer a + b et démontrer que 9a + 1 est un carré. Conclure.

Division euclidienne

Exercice : On donne deux entiers naturels a et b avec a > b. On effectue d'une part la division euclidienne de a par (a – b), d'autre part la division euclidienne de b par (a – b). Comparer les quotients et les restes de ces deux division.

Exercice : a, b et c sont trois entiers naturels. Soit q le quotient de la division euclidienne de a par b, et q' le quotient de la division euclidienne de q par c. Démontrer que q' est le quotient de la division euclidienne de a par bc.

PGCD, PPCM

Exercice : Trouver tous les couples de nombres entiers positifs dont le pgdc soit égal à 12 et la somme à 60. On s'assurera qu'on en n'a pas oublié.

Exercice : Soit d le pgdc de deux entiers a et b. Déterminer le pgdc de A = 15a + 4b et B = 11a + 3b.

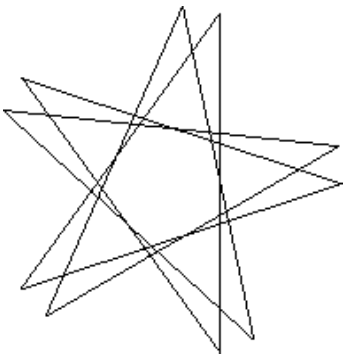
Exercice : a et b sont deux entiers relatifs. On considère A et b tels que A = pa + qb et B = ra + sb avec ps – qr = 1. démontrer que PGCD(a,b) = PGCD(A,B) (Queysanne et Revuz, manuel de Term C Nathan, 1972)

Exercice : Le ppcm de deux entiers naturels est 216. L'un des deux nombres est 72. Trouver toutes les valeurs possibles de l'autre.

Exercice : a et b sont deux entiers relatifs. Démontrer l'équivalence des deux affirmations suivantes : " a et b sont premiers entre eux" ; " a + b et ab sont premiers entre eux".

Exercice : Trouver les nombres à la fois congrus à 1 modulo 3 et congrus à 2 modulo 7. (**éventuellement à titre d'activité guidée en classe)**.

Exercice : n points divisent un cercle en n arcs de même longueur. A est un de ces n points. p étant un naturel compris entre 1 et n – 1, on forme un polygone régulier (généralement étoilé), en joignant A au point A_1 situés p points plus loin, puis enjoignant A_1 à A_2 situés p points plus loin et ainsi de suite. La suite A_1 , A_2 ,…finit par se refermer. Combien comporte-t-elle alors de points ?



Décomposition en produit de facteurs premiers

Exercice : * $(\ln 3) / (\ln 2)$ est-il un rationnel ? Justifiez.

* Si p et q sont deux nombres premiers distincts, démontrer que $(\ln p) / (\ln q)$ n'est pas un nombre rationnel.

* a et b sont deux entiers. Démontrer que $(\ln a) / (\ln b)$ est égal à la fraction irréductible m / n (m et n entiers naturels) ssi il existe un entier naturel c tel que : $a = c^m$ et $b = c^n$.

Nombres premiers entre eux

Exercice : Démontrer que tout entier naturel n supérieur ou égal à 7, l'intervalle] 1 , n – 1 [contient au moins un nombre premier avec n.

Indication : On pourra successivement traiter les trois cas : n est impair, n est une puissance de 2, puis n n'est ni impair ni une puissance de 2. Si n est impair, on peut prendre m = n – 2. Si n est une puissance de 2, on peut prendre m = n – 3. Sinon, n s'écrit sous la forme : $2^k.i$, avec i impair et $k \geq 1$. Posons m = i + 2. m est premier avec i et avec 2, donc m est premier avec $2^k.i = n$. De plus, $n \leq m$ conduit à m = 6, ce qui est exclus. C'est donc que m < n. m est donc bien le nombre recherché.

Systèmes de numération

Multiplication de grands nombres : Effectuer le produit : $(a_1.10^n + a_0).(b_1.10^n + b_0)$.

Appliquer cela pour trouver le produit de deux très grands nombres.

Exercice : Soit le nombre 120 450. Par quels chiffres remplacer les deux zéros pour que le nouveau nombre obtenu soit divisible par 99 ?

Variante Soit le nombre de 18 chiffres : 120 230 340 450 560 670. Par quels chiffres remplacer les six zéros pour que le nouveau nombre obtenu soit divisible par 99 ?

Exercice : Trouver tous les nombres N s'écrivant à la fois xyz en base 7 et zyx en base 11.

En revenant à la définition d'une base de numération, on obtient l'équation équivalente : y = 6(2x - 5z), qui implique que y est multiple de 6, donc égal à 0 ou 6. On trouve alors aisément les triplets solutions : (0,0,0) ; (5,0,2) ; (3,6,1)

Autre démarche : D'après l'écriture en base 7, ce nombre est inférieur ou égal à $7^3 = 343$. Mais alors, son écriture en base 11 implique que z égale 0, 1, ou 2. Si z = 0, on arrive à l'égalité : y = 12x qui entraîne que N = 0 ; si z = 1, on a : 12x – y = 30, d'où x = 3, y = 6 qui conviennent. Si z = 2, on a 12x – y = 60, d'où x = 5 et y = 0.

Exercice : **Démontrer que le carré d'un entier ne peut pas admettre une écriture en base 10 se terminant (à droite) par deux chiffres impairs.**
démonstration : Le carré d'un nombre pair se termine à droite par un nombre pair, donc ne peut certainement pas avoir cette forme. Examinons maintenant le carré d'un nombre impair.
Remarquons d'abord que pour u = 1,3,5,7,9, le carré de u est de la forme $u^2 = 20 x + c$, c et x étant entiers naturels, et c élément de [[1,9]], impair. Autrement dit, le chiffre des dizaines de u^2 est pair.
Mais tout entier naturel impair n peut s'écrire : n = 10d + u, u valant 1,3,5,7, ou 9, et D étant un entier naturel.
Il s'ensuit : $n^2 = (10d + u)^2 = 100d^2 + 20du + u^2 = 100d^2 + 20du + 20x + c = 20(5d^2 + du + x) + c$ avec c élément de [[1,9]].
Donc le chiffre des dizaines de n^2 est pair. Ceci achève la démonstration.

Autre démonstration modulo 4. Nous n'avons à examiner que le cas du carré d'un nombre naturel impair n. Pour tout entier naturel n impair, n^2 est congru à 1 modulo 4.
Or, si a est le chiffre des dizaines de n^2, et b son chiffre des unités, il est classique que n^2 est congru à 10a + b et à 2a + b modulo 4. Donc 2a + b est congru à 1 modulo 4.
Mias le chiffre des unités de l'écriture de n^2 en base 10 ne peut être que 1, 5 ou 9. On voit bien que ce chiffre b est congru à 1 modulo 4.
On en déduit que 2a est congru à 0 modulo 4, et donc que a est pair.

Algorithme d'Euclide : (Queysanne et Revuz, op.cit., 2.50 page 103)
Soit a un entier supérieur ou égal à 2. i étant un entier naturel, on note A_i le nombre : $a^i – 1$.
- Démontrer que $A_{(m + k)}$ et A_k ont même reste dans la division par A_m.
- En déduire que si m a pour reste r dans la division par m, alors :
  A_m a pour reste A_r dans la division par A_m.
- En déduire que si m et n ont pour PGDC : d, alors :
  A_m et A_n ont pour PGDC : A_d.
- M est le nombre qui en base 10 s'écrit par le chiffre 9 répété 4 679 fois. n est le nombre qui en base 10 s'écrit par le chiffre 9 répété 2 519 fois. Déterminer le PGDC de M et N.

6. Références

6.1. BIBLIOGRAPHIE

• **Initiation à l'arithmétique**, IREM de Bordeaux, groupe arithmétique et géométrie (paru ?)
• **Secrets de nombres** , "Tangente" Hors-Série n° 6, Éditions Archimède, + suppléments hors série J046
• Un cours de l'IREM de Marseille, téléchargeable à l'adresse jointe au 6.2.
• Le livre des nombres, Conway et Guy, chez Eyrolles
• Le dictionnaire Penguin des Nombres Curieux, Welles, Eyrolles.

Calendriers : de nombreux articles de J. Lefort, sur le bulletin "l'ouvert" . Voir l'adresse électronique de l'IREm de Strasbourg ci-dessous.
Calendriers et Chronologie, Parisot et Suagher, Masson.

Cryptographie : Voir Tangente , n° 37, n° 3, n° 5.

Les Arabes, durant notre Moyen Âge, se passionnaient pour l'arithmétique et énonçaient des théorèmes que redécouvrirent les mathématiciens européens de la Renaissance. Voir pour cela : **Histoire des sciences arabes, tome 2,** Rashi Rashed, Seuil.

Voir aussi, sur les nombres premiers ou parfaits, les deux derniers chapitres de **Histoire des mathématiques, Histoires de Problèmes,** Commission InterIrem, Ellipses.

6.2 . Sur le WEB

J'ai trouvé (pas exhaustif !)

Des exercices intéressants d'un collègue de l'Académie de Nice.
http://www2.ac-nice.fr/second/discip/maths/coin/textes/arith/exercices/codage.htm

Un abord algorithmique très intéressant de Jacques Sosset. (Ac. de Toulouse).
http://www.ac-toulouse.fr/math/chantier/ts_2_2.htm

Pour télécharger l'ouvrage de l'IREM de Marseille :
www.irem.univ-mrs.fr/arithmetique/Arith_TS.ps

adresse de l'IREM de Strasbourg :
http://www-irma.u-strasbg.fr/~irem/

Deux sites internet à retenir pour l'histoire des maths :

Université de St-Andrews : http://www-groups.dcs.st-and.ac.uk/~history/index.html

Élements d'Euclide (en anglais) : http://aleph0.clarku.edu/~djoyce/java/elements/elements.html

GÉOMÉTRIE : Pavages du plan, l'œuvre d'Escher :
Le site s'appelant **:** Totally Tessellated
http://library.advanced.org/16661/escher/

Annexe 1

Dans cette annexe, nous proposons : – Une démonstration directe du théorème de Gauss, par récurrence (on peut aisément l'adapter en démonstration par l'absurde et plus petit élément supposé).

– Une démonstration de l'unicité de la décomposition primaire à partir du théorème de Gauss.

– Une démonstration directe de l'unicité de la décomposition primaire, dans laquelle j'ai essayé de simplifier un peu la démonstration de l'IREM de Bordeaux, ou du Terracher, issue d'un ouvrage de Hardy et Wright.

1. Démonstration directe, par récurrence, du théorème de Gauss

Théorème de Gauss

Soient a, b, c trois entiers relatifs. Si a divise bc, et si a est premier avec b, alors a divise c.

DémonstrationNous allons d'abord démontrer par récurrence que le théorème est vrai dans le cas où a, b et c sont positifs.

Pour cela, notons **P(n)**, pour n élément de **N,** la propriété suivante :

Pour tous entiers a, b, c de **N**, tels que
- a premier avec b
- a divise bc
- bc = n,

on a : **a divise c**.

>> Démontrons P(0).

Supposons que Si • a premier avec b • a divise bc • bc = 0. Alors b = 0 ou c = 0.

• Si b = 0, comme a est premier avec b, a = 1. Donc a divise c.

• Si c = 0, alors a divise c.

a divise obligatoirement c, donc P(0) est vrai.

>> P(1) est évident (Car dans ce cas, a = b = c = n = 1)

>>Soit N élément de $\mathbf{N}^*$. Supposons que P(n) est vrai pour tout entier naturel n inférieur ou égal à N, et déduisons-en P(N + 1).

Soient donc des entiers a, b, c de $\mathbf{N}^*$, tels que **• a premier avec b • a divise bc • bc = N + 1.**

De trois choses l'une : a = b ou a < b ou a > b.

* Si a = b, alors, a étant premier avec b, on a : a = b = 1. Donc a divise c.

* Si a < b, posons e = b – a. a est premier avec b, donc **a est premier avec e** = b – a. De plus ec s'écrit ec = (b – a)c = bc – ac. **Donc a divise ec**, et aussi : ec < ac = N + 1, d'où **ec ≤ N**. On peut donc appliquer l'hypothèse de récurrence : On en déduit que a divise c.

* Si a > b, posons e = a – b. a divise bc, donc il existe un entier positif non nul k tel que bc = ak. b divise donc ak. De plus ek s'écrit : ek = (a – b)k = ak – bk. On en déduit que **b divise ek**, et que l'on a : ek < ak = N + 1. D'où **ek ≤ N**. Enfin, b est premier avec a, donc **b est premier avec e**. On peut donc appliquer l'hypothèse de récurrence : On en déduit que b divise k. Il existe donc un entier l tel que k = bl. On a alors : bc = abl, d'où c = al. On en déduit que a divise c.

Dans les trois cas, a divise c. Alors P(N + 1) est vraie.

>> Par récurrence, on conclut que P(n) est vraie pour tout entier n de **N**. On en déduit aisément que le théorème de Gauss est vrai sous l'hypothèse : a, b, c entiers relatifs. Il suffit de considérer les valeurs absolues et d'utiliser le cas " entiers naturels" .

2. Démonstration de l'unicité de la décomposition primaire, à partir du théorème de Gauss.

Lemme : Soit p un nombre premier et b_1, b_2, …b_k des nombres entiers relatifs. Si p divise le produit $b_1.b_2.…b_k$, alors p divise l'un des entiers b_1, b_2, …b_k.
démonstration : Immédiate par récurrence sur k grâce au théorème de Gauss.

Théorème:

Tout nombre entier naturel n différent de 1 admet un diviseur premier (de plus, si n n'est pas nul, n admet un diviseur premier dont le carré est inférieur ou égal à n).

Théorème :

Tout nombre entier naturel n supérieur ou égal à 2 admet une décomposition en produit de facteurs premiers sous la forme : $n = p_1 . … .p_k$, chacun des facteurs p_1, … p_k étant un nombre premier.

De plus, la décomposition ordonnée de n en produit de facteurs premiers, sous la forme : $n = p_1 .p_2 . … .p_k$, avec $p_1 \leq p_2 \leq … \leq p_k$, est unique. C'est-à-dire que si l'on a : $n = p_1 .p_2 . … .p_k = q_1 .q_2 . … .q_l$, avec $p_1 \leq p_2 \leq … \leq p_k$ et $q_1 \leq q_2 \leq … \leq q_l$, alors obligatoirement : l = k et pour tout i de [[1 , k]] : $p_i = q_i$.

Deux décompositions (non forcément ordonnées) d'un nombre entier naturel n supérieur ou égal à 2 sont donc identiques à l'ordre des facteurs près.

Démonstration de l'existence : sans difficulté par récurrence à partir du théorème précédent.

Démonstration de l'unicité à partir du lemme :

Nous allons effectuer un raisonnement par récurrence.
n étant un entier supérieur ou égal à 2, on note P(n) la proposition suivante : la décomposition de n est unique.

• P(2) est évidente

• N étant un entier supérieur ou égal à 2, supposons que P(n) est vraie pour tout n de [[2 , N]], et montrons que P(N + 1) est vraie.

Considérons deux décompositions ordonnées de N + 1 :

$N + 1 = p_1 . … .p_k = q_1 . … .q_l$, avec $p_1 \leq … \leq p_k$ et $q_1 \leq … \leq q_l$.

On peut supposer que $k \leq l$.

>> Si k = 1, l'unicité de la décomposition de N + 1 est immédiate.

>> Supposons maintenant : $k \geq 2$.

D'après le lemme : p_1 divise l'un des nombres premiers q_i . Donc $p_1 = q_i$, de dernier nombre étant supérieur ou égal à q_1 . Donc $p_1 \geq q_1$. Mais de même, q_1 divise p_1. p_2 …p_k . Donc q_1 divise l'un des nombres premiers q_j . Donc $q_1 = p_j$, de dernier nombre étant supérieur ou égal à p_1 . Donc $q_1 \geq p_1$. Donc $p_1 = q_1$. S'ensuit : $p_2 . … .p_k = q_2 . … .q_l$, ce nombre étant strictement inférieur à N + 1. Alors d'après l'hypothèse de récurrence : k – 1 = l – 1 et : $p_2 = q_2 … p_k = q_k$.

S'ensuit : k = l et pour tout i de [[1,k]] : $p_i = q_i$ .Donc P(N + 1) est vraie.

• Nous avons donc démontré, par récurrence, l'unicité.

3. Démonstration directe de l'unicité de la décomposition d'un entier en produit de facteurs premiers

Nous allons démontrer par l'absurde l'unicité de la décomposition ordonnée d'un entier supérieur ou égal à 2 en produit de facteurs premiers.

On note E l'ensemble des entiers supérieurs ou égaux à 2 admettant deux décompositions ordonnées distinctes.

Supposons que E n'est pas vide (pour arriver à une impossibilité).

Alors E admet un plus petit élément N. N admet deux décompositions ordonnées distinctes en produit de facteurs premiers : Notons, parmi ces deux décompositions ordonnées de N :

$N = p_1 …. .p_k$ celle qui commence par le plus petit nombre premier, et $N = q_1 . … .q_l$, l'autre décomposition avec, donc, $p_1 \leq q_1$. On a : $p_1 \leq … \leq p_k$ et $q_1 \leq … \leq q_l$.

Remarquons qu'il est impossible que k ou l soit égal à 1.

De deux choses l'une : Ou bien $p_1 = q_1$, ou bien $p_1 < q_1$.

• Si $p_1 = q_1$, alors $p_2 . \ldots . p_k = q_2 . \ldots . q_l$. Ce nombre est compris au sens strict entre 1 et N. Donc il n'appartient pas à E et admet une décomposition ordonnée unique : $k - 1 = l - 1$ et : $p_2 = q_2$,… $p_k = q_k$. Mais alors les deux décompositions de N sont identiques : Nous arrivons à une contradiction.

• Si $p_1 < q_1$, notons D : $q_1 - p_1$;

Alors $N = p_1p_2.\ldots.p_k = (p_1 + D)q_2 \ldots q_l$, d'où : $p_1(p_2.\ldots.p_k - q_2 \ldots q_l) = D\, q_2 \ldots q_l = N'$, ce nombre étant strictement inférieur à N et non nul.

Décomposons la parenthèse du premier terme ainsi que D en produits de facteurs premiers, respectivement $r_1 \ldots . r_{m'}$ et $d_1 \ldots . d_m$. Alors :

$p_1.r_1 \ldots . r_{m'} = d1 \ldots . d_m q_2 \ldots q_l = N'$. On a $0 < N' < N$, donc la décomposition de N' en produit de facteurs premiers est unique. Donc p_1 est l'un des nombres di, ou bien l'un des nombres qi.

Dans le premier cas, p_1 divise q_1, et on arrive à une contradiction car on a supposé: p1 < q1.

Dans le deuxième cas $p_1 = q_i$ avec $q_i \geq q1$. D'où $p_1 \geq q1$, et on arrive de nouveau à une contradiction.

Il est donc impossible que E ne soit pas vide. Donc E est vide. Il n'existe donc pas d'entier naturel supérieur ou égal à 2 admettant deux décompositions ordonnées distinctes en produit de facteurs premiers.

Annexe 2

D'après le Groupe de Travail Disciplinaire :

" Il est opportun de dresser des tables d'addition ou de multiplication de Z/nZ dans quelques cas particuliers pour des activités d'études de lignes, de colonnes… par exemple, dans la table de multiplication de Z/6Z, étudier la ligne des multiples de la classe 4 : valeurs atteintes, produits trouvés plusieurs fois, valeurs non atteintes. Même étude pour les multiples de la classe 5. dans la table de multiplication de la classe 7, étudier les mêmes questions."

Proposition de mise en œuvre :

Exercice pouvant motiver cette table :

Restes dans la division de par 6 — de y → / de xy / de x ↓ . ↘	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

• Dresser la table de multiplication des restes modulo 6.

Grâce à cette table, résoudre dans $\mathbf{Z} \times \mathbf{Z}$: $xy \equiv 2$ [6] ou : $xy \equiv 1$ [6] .

Ou si l'on préfère : Quels sont les entiers relatifs x et y tels que le reste de la division euclidienne de xy par 6 soit égal à 2 (resp : le reste soit égal à 1) ?

• On dispose de deux urnes, chacune contenant les entiers compris entre 0 et 5. On tire au hasard un carton de chaque urne. On effectue leur produit. Pierre parie que le reste de la division euclidienne par 6 de ce produit est 3. Paul parie que ce sera 2.

Qui a le plus de chance de gagner ?

• Comment expliquer les restes décroissants : 5,4,3…1 dans la dernière ligne de cette table ?

[Réponse : 5 est congru à (– 1) donc les différents produits 5x1, 5x2…5x5 vont être respectivement congrus modulo 6 à : (– 1), (– 2), (– 3)…(– 5), et donc donneront comme restes modulo 6 : 6 – 1, 6 – 2, …6 – 5]

Questions : Que pensez-vous de la fréquence de chaque reste non nul dans ce tableau ? Expliquez pourquoi.

Remarquer que de nouveau la dernière ligne contient zéro, suivi de tous les restes modulo 7 dans l'ordre décroissant.

Quelle particularité présente la diagonale de cette table ? Expliquez cette particularité.

Restes dans la division de par 7 — de y → / de xy / de x ↓ . ↘	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Généralisations

• On considère la **table de multiplication des restes modulo 15.** Cependant on ne dressera pas cette table, ce qui serait trop long. On s'intéresse seulement à certaines propriétés des lignes.

– Démontrer que sur la ligne de cette table correspondant à **8**, les nombres sont tous distincts deux à deux. [En effet : Si $8x \equiv 8y$ [15] , alors $8(x – y) \equiv 0$ [15] , donc 15 divise x – y donc x = y (si x et y appartiennent à [[0,14]].]

– En déduire que sur cette ligne de cette table correspondant à **8**, chaque reste modulo 8 figure une et une seule fois.

Ou bien : À la place de cette dernière question : Démontrer qu'il existe un entier relatif x tel que $8x \equiv 1$ [15]. [Se servir du théorème de Bezout].

En déduire que pour tout r élément de [[0,14]], il existe un entier relatif y tel que $8y \equiv r$ [15]. En déduire que la ligne 8 contient tous les restes modulo 15.

– On s'intéresse à la ligne correspondant au reste **5**. Caractériser les restes x et y modulo 15 tels que $5x \equiv 5y$ [15]. Utiliser cette propriété pour trouver les 10 premières colonnes de la ligne 5.

Réponse : $5x \equiv 5y$ [15] < = > 3 divise (x – y). D'où une période 3 sur la ligne 5, et ses 10 premières colonnes :

X	0	1	2	3	4	5	6	7	8	9	10
5	0	5	10	0	5	10	0	5	10	0	5…

– On s'intéresse maintenant à la ligne du reste **3**. Le reste 1 figure-t-il sur cette ligne ? Quels sont les restes susceptibles de figurer sur la ligne du reste 3 ? Démontrer qu'ils sont tous effectivement présents sur cette ligne. Caractériser les restes x et y modulo 15 tels que $3x \equiv 3y$ [15]. décrire la ligne 3.

– Démontrer que si a est premier avec 15, la ligne a contient tous les restes modulo 15 une et une seule fois.

– Cette propriété est-elle encore vraie si a n'est pas premier avec 15 ?

– <u>généralisation :</u> • On considère la **table de multiplication des restes modulo n.**

Quelles sont les lignes de cette table qui comprennent tous les restes modulo n, chacun d'eux une seule fois.

Quelles sont les lignes de cette table où certains restes sont répétés, et où d'autres sont absents ?

<u>Remarque</u> : Dans le cas où n est premier, le résultat que nous venons de mettre en évidence sur la ligne a (non nul) de la table de multiplication modulo n permet de démontrer le " petit" **théorème de Fermat**.

Reste modulo n de a^p .

Dans le même ordre d'idée, il convient sans doute de donner, pour a fixé, les restes modulo n (fixé) de a^p, pour p entier variable. Ces tableaux constituent le fond même des exercices comme ceux donnés au début de ce paragraphe sur les congruences.

Remarquons aussi que seules des considérations de congruences permettent de calculer le reste de 2^{5000} modulo 9, par exemple.

Puissances modulo 9 (de 4, puis 5, puis 7, par exemple) .

Annexe 3

Le cryptage RSA (Rivet, Shamir, Adelman), à codage public

Le codage RSA est un codage de type **puissance.** Ce qui est frappant, c'est que sa méthode de codage peut être rendue publique, sans qu'on puisse en déduire une méthode de décodage.

Ce procédé considère d'abord un nombre N très grand, qui soit le produit de deux très grands entiers premiers : N = pq. Il est alors très difficile, à partit de N, de trouver les entiers premiers p et q. Mais nous allons donner un exemple avec des entiers beaucoup plus modestes. On prendra N = 91. Tout le monde connaît donc N, mais aussi un "nombre de codage", que nous noterons C, et prendrons ici égal à 29. Nous supposerons que notre message a déjà été chiffré en une suite de nombres compris entre 0 et 90 (par exemple, les rangs des lettres dans l'alphabet).

Le procédé de codage, que l'on va noter ici $\&$, va s'appliquer à un de ces nombres, noté x, pour donner un autre nombre de [[0,90]] . Plus précisément :

$\&(x) = y$ est le reste de la division euclidienne de $x^C = x^{29}$ par N = 91.

Ceci ne peut se faire que par un programme informatique, calculant à chaque fois le reste dans la division par 91.

Maintenant, considérons la partie "cachée", c'est-à-dire le décodage : Le décodage va être également de type puissance, reposant sur un "nombre de décodage" jalousement gardé : D. D a la propriété fondamentale suivante par rapport à C :

Pour tout réel x : $x^{CD} - x$ est divisible par N. (Propriété 1).

On définit la fonction de décodage $''$ de la façon suivante :

Pour tout nombre y de [[0,90]], $''(y) = z$ est le reste de la division euclidienne de x^D par N.

Question 1 : Démontrer dans le cas général que $''$ décode vraiment $\&$, à savoir que la propriété 1 entraîne que pour tout entier naturel x inférieur ou égal à (N – 1), $''(\&(x)) = x$.

Nous nous posons maintenant la question suivante : Quelle est la valeur ce D correspondant à C ? Comment l'auteur du codage a-t-il choisi les nombres C et D ?

Celui-ci connaît les deux nombres premiers p et q dont le produit est égal à N. Posons M = (p – 1)(q – 1). L'auteur du procédé de codage se sert de la propriété suivante :

Pour tout entier naturel x, $x^M - 1$ est divisible par N. (Propriété 2). Il choisit alors un nombre C quelconque premier avec M.

Question 2. En admettant la propriété 2, démontrer que tout nombre D tel que M divise CD – 1 vérifie la propriété 1. Justifier que si C est premier avec M, un tel nombre D existe.

Question 3 : On se place dans le cas particulier N = 91, C = 29. Trouver p et q. (Ceci ne serait pas possible avec p et q très grand.) Calculer M. Trouver une valeur possible pour D.

Question 4 : Décoder le message suivant.

Question 5 : À l'aide du petit théorème de Fermat, démontrer la propriété 2, dans le cas général.