



Classe de 7^{ème} C

Arithmétique

115 exercices corrigés

116 exercices proposés

Professeur
Sidi MAJOR

Série : mathématiques en mouvement

$$\text{Réussite} = \int_{\text{début}}^{\text{fin}} \left(\text{travail} / \text{méthode} \right) d(\text{temps})$$

« Aucune notion n'est plus relative que celle de réussite. Elle évoque un résultat, et n'a de sens que par comparaison. Sa mesure dépend du terme de référence, ou de la valeur à laquelle on accorde le plus de prix. Elle ressortit à plusieurs ordres. Pour telle personne elle se mesure en argent ou en pouvoir, pour telle autre en vertu ou en savoir, pour telle autre en beauté.

Quel que soit l'objet de prédilection de chacun, et sans chercher à savoir qui l'emporte du savant, du capitaine ou du poète, la réussite de l'un ou de l'autre repose d'abord sur un sentiment personnel et constitue l'incarnation de l'esprit de la formule intégrale citée ci-haut. »

Alain GIRARD, modifié
La réussite sociale
Que sais-je. PUF

Préambule

*« Les plus belles victoires,
les seules qui ne peuvent donner aucun regret,
sont celles que l'on fait sur l'ignorance »
Napoléon BONAPARTE*



Chers lecteurs, chères lectrices, comme il est impossible d'apprendre à nager sans plonger dans l'eau, il est également impossible d'apprendre à résoudre des problèmes de mathématiques sans mettre la main à la patte autrement dit sans se confronter réellement à des exercices variés aussi bien au niveau du concept qu'au niveau de la difficulté.

Partant de cette conception, nous avons opté de donner :

- *un rappel de cours illustré par des exemples d'application mis en face à face du rappel;*
- *une batterie d'exercices corrigés, chapeautés de citations, proverbes ou maximes parfois humoristiques, empruntés à différentes cultures : arabes, africaines, asiatiques et européennes, pour attiser la sagacité du lecteur et briser la monotonie de la pesanteur naturelle du raisonnement scientifique. Ces corrigés sont accompagnés, pour certains, de commentaires et/ou de repères historiques qui replacent la notion étudiée dans son contexte heuristique ;*
- *une batterie d'exercices proposés à la résolution, de niveaux très variés, couvrant presque tous les types de questions susceptibles d'être posées dans le champ conceptuel étudié.*

Pour la batterie d'exercices corrigés, les corrigés ne doivent pas être consultés avant de faire une recherche hardie des solutions ; ces corrigés devront d'ailleurs constituer une source d'inspiration, un modèle de rédaction pour pouvoir s'attaquer efficacement aux exercices proposés.

La résolution d'un exercice ne peut et ne doit en aucun cas être une finalité en soi, mais c'est le cheminement intellectuel adopté dans la résolution qui doit être interpellé pour pouvoir dégager une démarche méthodologique générale pouvant être appliquée à toute une gamme de problèmes similaires. Donc l'objectif final de l'exercice de maths reste la capacité à débusquer des méthodes de résolution de problèmes qui se veulent transversales.

Il y a dans la résolution de tout problème de mathématiques, un peu d'une découverte. Un problème qui vous est soumis peut être sans prétention ; mais, s'il pique votre curiosité et fait entrer en jeu vos facultés d'invention et de créativité, si vous le résolvez par vous-même ... vous pouvez en ce moment-là connaître le charme de la découverte et en goûter le triomphe. Ce genre d'expérience peut déterminer le goût du travail intellectuel et laisser, tant sur l'esprit que sur le caractère, une empreinte indélébile qui façonnera la personnalité future de l'apprenti-chercheur que vous êtes.

D'autre part, vous remarquerez à travers les corrigés de ce manuel qu'une attention particulière a été accordée à la rédaction et à la rigueur du raisonnement. En effet, les mathématiques sont par excellence une science de la rigueur et donc tout compromis, aussi léger que soit-il, au détriment de cette rigueur compromettrait la quintessence même de la discipline. Dans ce domaine, je ne me généraïs point d'illustrer le haut niveau de rigueur des mathématiques, comparativement à toutes les autres sciences, à travers l'anecdote qui suit :

« Un mathématicien, un physicien et un ingénieur voyagent à travers l'Écosse. Ils voient un mouton noir par la fenêtre du train et immédiatement un dialogue s'instaure entre les trois voyageurs :

L'ingénieur : « Ah !, les moutons de ce pays sont noirs. » ;

Le physicien : « Hmm !, on peut plutôt dire que dans ce pays, il y a des moutons noirs. » ;

Le mathématicien : « Ah ! Non, tout ce qu'on peut dire c'est que dans ce pays, il y a au moins un mouton et que ce mouton-là a au moins un côté noir. »

Ah !, c'est clair qu'il y a ici une nette nuance dans la précision et telle est la vraie singularité des maths.

Ce 1^{er} tome s'adresse spécialement aux élèves de la classe de 7^{ème} C, aux professeurs de mathématiques, aux amateurs, mais aussi aux étudiants du 1^{er} cycle universitaire en MP et MI.

Enfin, je ne pourrai terminer sans exprimer, a priori, ma sincère gratitude à ceux et à celles qui prendront le soin de relever des remarques sur ce manuel tant sur la forme que sur le contenu et auront ensuite la gentillesse de me les faire parvenir sur l'adresse électronique « sidimajor@gmail.com » pour qu'ensemble, vous et moi, nous pourrions, par le biais de ce travail, apporter une mince contribution à l'enrichissement du patrimoine scolaire national.

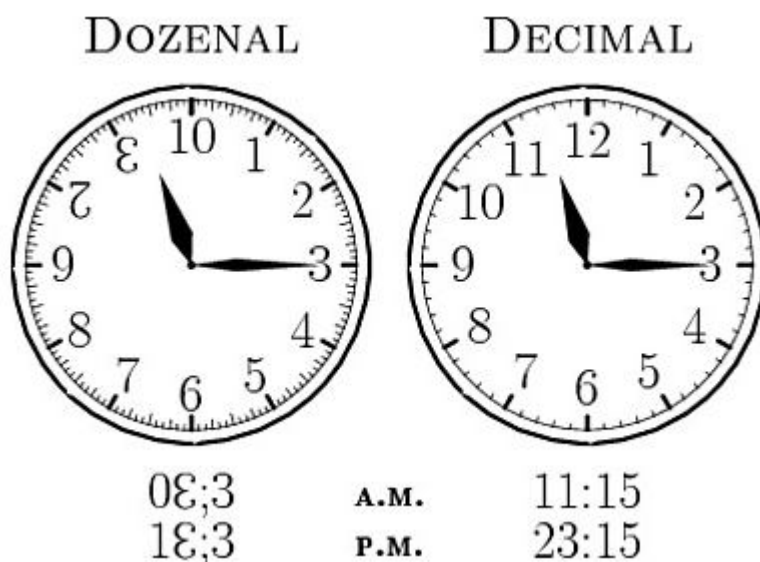
**Par l'auteur
Sidi MAJOR**

Dédicace



- à tous les collègues,
- aux élèves assoiffés de savoirs,
- à France Guerlain,
- à Tahya Tiki Demba.

Arithmétique



Citations - choc :

→ L'arithmétique, c'est être capable de compter jusqu'à vingt sans ôter ses chaussures.

Walt Disney.

→ La mathématique est la reine des sciences et l'arithmétique est la reine des mathématiques.

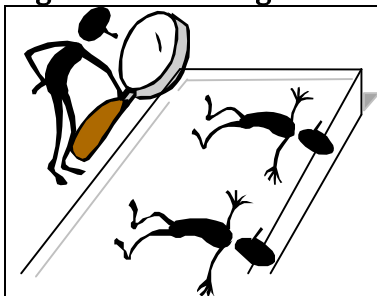
Carl Friedrich Gauss.

→ Doit-on dire « Tous les nombres premiers sont impairs sauf un », ou « Tous les nombres premiers sont impairs sauf deux » ?

Anonyme.

→ 13bis, est-ce un nombre pair ou impair ? R. Queneau.

Énigme : L'archéologue futé



Deux ethnologues découvrent un tombeau dans lequel il y a 2 êtres à l'état de chair (c'est-à-dire non décomposés, avec la peau sur les os). L'un des 2 s'écrie « Mais c'est Adam et Ève !! ».

Comment les a-t-il reconnus ?



I. Divisibilité dans $\mathbb{Z}$

Deux propriétés importantes de l'ensemble $\mathbb{N}$ des entiers naturels constituent le fondement de l'arithmétique élémentaire et peuvent être considérées comme axiomes constructifs de cette théorie :

- ① Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- ② Toute partie majorée de $\mathbb{N}$ est finie et réciproquement.

En outre, on ne peut que citer la propriété d'Archimède restreinte à $\mathbb{N}$:

«Étant donnés deux entiers $0 < a < b$, il existe un entier n tel que $b < na$ ».

Remarque :

$\mathbb{N}$, **ensemble des entiers naturels** : de l'italien naturale par Peano (1858-1932).

$\mathbb{Z}$, **ensemble des entiers relatifs** : de l'allemand Zahl, nombre et zahlen, compter par Dedekind (1831-1916).

Définition 1 :

a et b étant deux entiers relatifs, on dit que a est multiple de b s'il existe $k \in \mathbb{Z}$ tel que $a = k \times b$.

Définition 2 :

b étant un entier relatif non nul et a un entier relatif quelconque, on dit que « b divise a » et on notera $b|a$ s'il existe $k \in \mathbb{Z}$ tel que $a = k \times b$.

Remarque :

$$\text{« } b \text{ divise } a \text{ »} \Leftrightarrow \text{« } a \text{ est multiple de } b \text{ »}$$

Propriétés : a et b sont des entiers relatifs.

- ✓ Pour tout entier n , on a toujours $1|n$, $(-1)|n$.
- ✓ Pour tout entier non nul n , on a toujours $n|n$ et $(-n)|n$.
- ✓ Les seuls diviseurs de 1 ou (-1) sont 1 et (-1).
- ✓ Si $(a|b$ et $b|c)$ alors $a|c$ (propriété de transitivité).
- ✓ Si a / b et $b \neq 0$ alors $|a| \leq |b|$. Ainsi, tout entier non nul admet un nombre fini de diviseurs
- ✓ Dans $\mathbb{Z}$, on a : si $(a|b$ et $b|a)$ alors $a = b$ ou $a = -b$.
- ✓ Dans $\mathbb{N}$, on a : si $(a|b$ et $b|a)$ alors $a = b$.
- ✓ Si $(a|b$ et $a|c)$ alors $a|[ab + \beta c]$ pour tous entiers relatifs α et β .

Exemples d'application

Exemple 1

On veut déterminer les entiers relatifs $n \neq -2$ tels que $\frac{2n-29}{n+2}$ soit un entier.

- 1) Montrer que si n est solution alors $n+2$ divise 33.
- 2) Établir la liste des diviseurs de 33 dans $\mathbb{Z}$. En déduire les valeurs possibles de l'entier relatif n .
- 3) Conclure.

Corrigé

1) $\frac{2n-29}{n+2}$ entier $\Leftrightarrow n+2 \mid 2n-29$. Or $n+2 \mid n+2$ et donc par combinaison, on trouve :

$$n+2 \mid 2(n+2) - (2n-29) \text{ soit } n+2 \mid 33.$$

2) Les diviseurs de 33 dans $\mathbb{Z}$ sont : $-33, -11, -3, -1, 1, 3, 11, 33$.

3) On a : $\frac{2n-29}{n+2}$ entier $\Rightarrow n+2 \mid 33$ et donc :

$$n \in \{-35, -13, -5, -3, -1, 1, 9, 31\}.$$

Comme il s'agit juste d'une implication, il faut vérifier les valeurs obtenues une à une.

Pour $n = -35$, on a $\frac{2n-29}{n+2} = \frac{-99}{-33} = 3$ entier. Donc $n = -35$ est solution.

Ainsi, on peut vérifier pour toutes les valeurs de n .

Enfin, vous vérifierez que : $S = \{-35, -13, -5, -3, -1, 1, 9, 31\}$.

Exemple 2

Pour tout entier n , on pose : $a_n = 2n - 1$ et $b_n = 9n + 4$.

1) Déterminer un entier k indépendant de n tel que :

$$\text{Si } d \mid a_n \text{ et } d \mid b_n \text{ alors } d \mid k$$

2) En déduire la liste des diviseurs communs éventuels à a_n et b_n .

3) En déduire les diviseurs communs à 5 117 et 23 035. Quel est le PGCD des deux entiers 5 117 et 23 035 ?

Corrigé

1) $\begin{cases} d \mid a_n \\ d \mid b_n \end{cases} \Rightarrow d \mid -9a_n + 2b_n \text{ i.e } d \mid 17. \text{ Donc } k = 17.$

2) Selon la question 1), tout diviseur commun à a_n et b_n divise 17. Donc les diviseurs communs éventuels à a_n et b_n sont :

$$-17, -1, 1, 17.$$

3) Déterminons n tel que $a_n = 5117$ et $b_n = 23\,035$. On a :

$$a_n = 5117 \Leftrightarrow 2n - 1 = 5117 \Leftrightarrow n = 2559$$

On a bien $9 \times 2559 + 4 = 23\,035 = b_{2559}$. D'après 1), tout diviseur commun naturel à a_{2559} et b_{2559} est un diviseur de 17. Or, on vérifie bien que $17 \mid 5117$ et $17 \mid 23\,035$ et donc :

$$\text{PGCD}(5117, 23\,035) = 17.$$

II. Nombres premiers

Définition 1 :

Un entier naturel p est premier si et seulement si il possède exactement 2 diviseurs positifs distincts à savoir 1 et lui-même.

Théorèmes 1:

✓ *Tout entier naturel autre que 1 admet au moins un diviseur premier.*

Théorème 2 :

✓ *L'ensemble des nombres premiers est infini.*

Théorème 3 :

✓ *Tout entier naturel non premier (composé) admet au moins un diviseur premier p tel que $p^2 \leq n$*

Critère de primalité :

- ✓ *Si un entier naturel n n'est divisible par aucun nombre premier dont le carré est inférieur à n , alors n est un nombre premier.*
- ✓ *Application : Le crible d'Ératosthène.*

Décomposition en facteurs premiers

Théorème 4:

✓ *Tout entier naturel $n \geq 2$ s'écrit de manière unique sous la forme de sa décomposition en facteurs premiers $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ où $p_1 < \dots < p_k$ sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_k$ sont des entiers naturels non nuls.*

Théorème 5:

✓ *L'entier naturel $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ possède $(\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1)$ diviseurs dans l'ensemble $\mathbb{N}$ et $2(\alpha_1 + 1) \times (\alpha_2 + 1) \times \dots \times (\alpha_k + 1)$ diviseurs dans l'ensemble $\mathbb{Z}$.*

Exemples d'application

Exemple 3

- 1) Les nombres 251 et 221 sont-ils premiers ?
- 2) Décomposer en facteurs premiers les entiers suivants : 4992, 10 780. Quel est pour chacun des deux entiers le nombre de diviseurs.

Corrigé

- 1) On a : $\sqrt{251} \cong 15,84$. Les entiers premiers inférieurs à 15 sont : 2, 5, 7, 11 et 13. On peut vérifier que 251 n'est divisible par aucun entier de cette liste. Donc 251 est premier. De même, on procède avec 221 et on vérifie que 13 divise 221. Donc 221 n'est pas premier.
- 2) On effectue exhaustivement les divisions successives par les entiers premiers 2, 3, 5, ...

4992	2	Donc, on a :	10 780	2	Donc, on a :
2496	2		5390	2	
1248	2	4992 = 2⁷.3.13	2695	5	10780 = 2².5.7².11
624	2		539	7	
312	2		77	7	
156	2	Le nombre de	11	11	Le nombre de diviseurs de
78	2	diviseurs de 4992	1		10780 dans $\mathbb{N}$ est :
39	3	dans $\mathbb{N}$ est :			
13	13				$3 \times 2 \times 3 \times 2 = 36$
1					

Exemple 4

Trouver le plus petit entier naturel n dont le produit par 13 608 est :

- 1) Le carré d'un entier naturel ;
- 2) Le cube d'un entier naturel.

Corrigé

On peut vérifier aisément que $13\,608 = 2^3 \times 3^5 \times 7$.

- 1) Il faut multiplier 13 608 par un entier minimal n tel que les exposants de 2, 3 et 7 dans la décomposition de $13\,608n$ soient tous pairs. Donc, on remarque que $n = 2 \times 3 \times 7 = 42$.
- 2) Dans ce cas, il faut que les exposants de 2, 3 et 7 dans la décomposition de $13\,608n$ soient tous multiples de 3. Donc : $n = 3 \times 7^2 = 147$.

III. Division euclidienne dans $\mathbb{N}$ et dans $\mathbb{Z}$

Théorème 1 et définition (dans $\mathbb{N}$):

a et b sont des entiers naturels, b est non nul, il existe un unique couple $(q; r)$ d'entiers positifs tel que :

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

q est le quotient et r le reste de la division euclidienne de a par b .

Définition (dans $\mathbb{Z}$):

a et b sont des entiers relatifs, b est non nul, il existe un unique entier relatif q et un unique entier positif r tels que : $a = bq + r$ et $0 \leq r < |b|$

IV. Congruence dans $\mathbb{Z}$

Définition 1:

On dit que deux entiers relatifs a et b sont congrus modulo n (où n est entier ≥ 2) si et seulement si il existe un entier k tel que $b = k \times n + a$ (attention ce n'est pas une division euclidienne).

On écrit $a \equiv b [n]$.

Définition 2:

$a \equiv b [n] \Leftrightarrow a - b$ est un multiple de n .

Définition 3:

$a \equiv b [n] \Leftrightarrow a$ et b ont le même reste dans la division euclidienne par n .

Théorème 1 :

Si le reste de la division euclidienne de a par n est égal à r alors $a \equiv r [n]$.

En particulier si n divise a alors $a \equiv 0 [n]$.

Propriété de transitivité :

Si $a \equiv b [n]$ et $b \equiv c [n]$ alors $a \equiv c [n]$.

Règles de calculs :

① Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a + c \equiv b + d [n]$

(compatibilité de la congruence avec l'addition)

② Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a - c \equiv b - d [n]$.

③ Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a \times c \equiv b \times d [n]$

(compatibilité de la congruence avec la multiplication)

④ Si $a \equiv b [n]$ alors $a^p \equiv b^p [n]$. (p est un entier positif)

Remarque : Les règles marchent avec le même modulo $[n]$; les divisions ne marchent pas !

Exemples d'application

Exemple 5

- 1) Montrer que tout entier relatif n peut s'écrire nécessairement sous l'une des trois formes $3k$, $3k + 1$ ou $3k + 2$.
- 2) Le reste de la division euclidienne de l'entier naturel a par 18 est 16. Quel est le reste de la division euclidienne de a par 9 ? par 6 ?
- 3) Dans la division euclidienne de 1512 par un entier naturel non nul b , le quotient est 17 et le reste r . Déterminer les couples solutions (b, r) .

Corrigé

- 1) En divisant n par 3, le reste est soit 0, 1 ou 2. Donc n s'écrit nécessairement sous l'une des trois formes.
- 2) On a : $a = 18q + 16$ et donc quotient = q et reste = 16.
Division euclidienne par 9 :
 $a = 18q + 16 = 9(2q) + 9 + 7 = 9(2q + 1) + 7$ et donc :
quotient = $2q + 1$ et reste = 7
Division euclidienne par 6 :
 $a = 18q + 16 = 6(3q) + 6 \times 2 + 4 = 6(3q + 2) + 4$ et donc :
quotient = $3q + 2$ et reste = 4
- 3) On a : $1512 = 17b + r$ avec $0 \leq r < b$ et en rajoutant $17b$ à chaque membre de l'inégalité du reste, on obtient : $17b \leq 17b + r < 18b$. Soit, en remplaçant $17b + r$ par 1512 :
 $17b \leq 1512 < 18b$.
Cette double inégalité conduit à : $\frac{1512}{18} < b \leq \frac{1512}{17}$ ou encore $b = 85, 86, 87$ ou 88.
On a : $r = 1512 - 17b$ ce qui donne les couples (b, r) solutions :
 $(85, 67), (86, 50), (87, 33), (88, 16)$

Exemple 6

- 1) Montrer que 17 divise $35^{228} + 84^{501}$.
- 2) Soit n un entier quelconque. Quels sont les restes possibles de n^2 et n^3 dans la division euclidienne par l'entier 5 ?

Corrigé

- 1) On a : $35 \equiv 1 [17]$ et $84 \equiv 16 [17]$. Or $16 \equiv -1 [17]$ d'où par transitivité $84 \equiv -1 [17]$.
- 2) Donc $35^{228} + 84^{501} \equiv 1^{228} + (-1)^{501} [17]$ et par suite $35^{228} + 84^{501} \equiv 0 [17]$ c'est-à-dire 17 divise $35^{228} + 84^{501}$.
- 3) Il est souvent utile de présenter les résultats sous forme de tableau pour les congruences :

$n \equiv \dots [5]$	0	1	2	3	4
$n^2 \equiv \dots [5]$	0	1	4	4	1
$n^3 \equiv \dots [5]$	0	1	3	2	4

V. PGCD – PPCM

Notation:

On notera $D(a)$ l'ensemble des diviseurs de a et $D(a; b)$ l'ensemble des diviseurs communs à a et b .

Définition 1:

Le $PGCD(a; b)$, noté encore $a \wedge b$, est le plus grand élément de $D(a; b)$.

Définition 2:

Le $PPCM(a; b)$, noté encore $a \vee b$, est le plus petit commun multiple strictement positif de a et b .

Théorème 1:

Si $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$ avec α_i et β_i entiers pouvant être nuls (si par exemple $\alpha_i = 0$, le facteur p_i ne figure pas dans la décomposition de a) alors :

$$PGCD(a; b) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \dots \times p_k^{\min(\alpha_k, \beta_k)}$$

$$PPCM(a; b) = p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \dots \times p_k^{\max(\alpha_k, \beta_k)}$$

Propriétés :

Pour tous entiers relatifs a , b et k , on a :

① $PGCD(a; 0) = |a|$.

② Si $b|a$ alors $PGCD(a; b) = |b|$.

③ Si r est le reste dans la division euclidienne de a par b alors :

$$PGCD(a; b) = PGCD(b; r).$$

④ $PGCD(a; b) = PGCD(|a|; |b|)$.

⑤ $PGCD(ka; kb) = |k| \times PGCD(a; b)$.

Propriétés :

① Tout diviseur de a et b est un diviseur de $PGCD(a; b)$.

② Tout diviseur de $PGCD(a; b)$ est un diviseur de a et b .

③ Si $g = PGCD(a; b)$ alors $D(a; b) = D(g)$.

④ $PGCD(a; b) \times PPCM(a; b) = |a| \times |b|$.

Conséquence: Si $a \wedge b = 1$ alors $PPCM(a; b) = |a| \times |b|$.

Exemples d'application

Exemple 7

Déterminer de deux façons différentes $d = \text{PGCD}(390; 525)$.

Corrigé

→ **Par l'algorithme d'Euclide**

Cet algorithme de la détermination du PGCD de deux entiers a et b repose sur les deux propriétés du cours :

③ Si r est le reste dans la division euclidienne de a par b alors :

$$\text{PGCD}(a; b) = \text{PGCD}(b; r).$$

① Si a est un entier relatif non nul alors : $\text{PGCD}(a; 0) = |a|$.

Ainsi, en divisant $a = 525$ par $b = 390$: $525 = \underbrace{1}_{=q} \times 390 + \underbrace{135}_{=r}$, on conclut que :

$$d = \text{PGCD}(390; 525) = \text{PGCD}(390; 135).$$

De même : $390 = 2 \times 135 + 120$ et donc $\text{PGCD}(390; 135) = \text{PGCD}(135; 120)$.

Si on poursuit, on obtient :

$135 = 1 \times 120 + 15$ et donc $\text{PGCD}(135; 120) = \text{PGCD}(120; 15)$;

$120 = 8 \times 15 + 0$ et donc $\text{PGCD}(120; 15) = \text{PGCD}(15; 0) = 15$.

Enfin, on trouve $d = \text{PGCD}(390; 525) = 15$.

Disposition pratique :

$$525 = 1 \times 390 + 135$$

$$390 = 2 \times 135 + 120$$

$$135 = 1 \times 120 + \boxed{15}$$

$$120 = 8 \times 15 + 0$$

Et donc le PGCD recherché est le dernier reste non nul (ici 15).

→ **Par la décomposition en facteurs premiers**

On peut établir aisément que :

$$390 = 2 \times 3 \times 5 \times 13 \quad \text{et} \quad 525 = 3 \times 5^2 \times 7$$

Et par suite $\text{PGCD}(390; 525) = 3 \times 5 = 15$.

Remarque :

Le PPCM(a ; b) peut être déterminé à partir de l'égalité :

$$\text{PPCM}(a, b) = \frac{|a| \times |b|}{\text{PGCD}(a; b)}$$

Ainsi, dans notre exemple, $\text{PPCM}(390; 525) = \frac{390 \times 525}{15} = 13\,650$.

VI. Théorèmes de Bézout et de Gauss

Définition :

Deux entiers relatifs sont premiers entre eux si leur PGCD est égal à 1.

Théorème 1 (de Bézout):

Soient a et b des entiers relatifs.

$a \wedge b = 1 \Leftrightarrow$ Il existe 2 entiers u et v tels que $au + bv = 1$.

Théorème 2 :

Soit a et b deux entiers naturels.

$$a \wedge b = d \Leftrightarrow \exists a' \text{ et } b' \in \mathbb{N} \text{ tels que } \begin{cases} a = a'd \\ b = b'd \\ a' \wedge b' = 1 \end{cases}$$

Théorème 3 (Identité de Bézout):

Si $a \wedge b = d$ alors il existe 2 entiers u et v tels que $au + bv = d$, la réciproque est fausse, il faut rajouter une condition :

Si $(au + bv = d \text{ et } d \text{ divise } a \text{ et } b)$ alors $a \wedge b = d$.

Théorème 4 (de Gauss):

Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise l'entier c .

Soit : Si $\begin{cases} a \text{ divise } b \times c \\ a \wedge b = 1 \end{cases}$ alors $(a \text{ divise } c)$

Conséquences (lemme d'Euclide) :

Si $\begin{cases} a \text{ est premier} \\ a \text{ divise } b \times c \end{cases}$ alors $(a \text{ divise } b) \text{ ou } (a \text{ divise } c)$

Si $\begin{cases} a \text{ et } b \text{ divisent } c \\ a \wedge b = 1 \end{cases}$ alors $a \times b \text{ divise } c$

Théorème 5 (petit théorème de Fermat):

Soit a un entier relatif et p un entier naturel.

Si $\begin{cases} p \text{ est premier} \\ p \text{ ne divise pas } a \end{cases}$ alors $a^{p-1} \equiv 1 \pmod{p}$ (c'est-à-dire $p \mid a^{p-1} - 1$)

Théorème 6 (de Wilson):

Pour tout entier naturel p , on a l'équivalence :

$$p \text{ premier} \Leftrightarrow (p-1)! \equiv -1 \pmod{p}$$

Exemples d'application

Exemple 8

On sait déjà d'après l'exercice d'application n°7 que $\text{PGCD}(390; 525) = 15$. Le théorème 3 de l'identité de Bézout affirme l'existence de deux entiers relatifs u et v tels que $525u + 390v = 15$. Déterminer les deux coefficients u et v (**Algorithme d'Euclide étendu**).

Corrigé

On effectue les divisions successives jusqu'à l'obtention du PGCD :

$$525 = 1 \times 390 + 135$$

$$390 = 2 \times 135 + 120$$

$$135 = 1 \times 120 + \boxed{15}$$

$$120 = 8 \times 15 + 0$$

Puis on remonte les divisions en exprimant chaque reste comme combinaison linéaire des entiers qui l'ont généré:

$$15 = 135 - 1 \times 120$$

$$= 135 - 1 \times (390 - 2 \times 135)$$

$$= -1 \times 390 + 3 \times 135$$

$$= -1 \times 390 + 3 \times (525 - 1 \times 390)$$

$$= 3 \times 525 + (-4) \times 390$$

Et donc $u = 3$ et $v = -4$.

Disposition pratique donnant le PGCD et les coefficients u et v :

On commence par construire le tableau suivant à deux lignes qu'on prolongera si besoin en est :

$$\begin{array}{l} L_1 \rightarrow \\ L_2 \rightarrow \end{array} \begin{array}{|c|c|c|} \hline a & 1 & 0 \\ \hline b & 0 & 1 \\ \hline \end{array}$$

On complète le tableau vers le bas par la ligne $L_3 = L_1 - qL_2$ où q est le quotient de la division euclidienne de a par b . On continue ainsi le procédé et on arrête dès qu'on obtient une ligne dont le 1^{er} élément est nul. Enfin, les deux dernières lignes seront de la forme :

d	u	v
0	x	y

où $d = a \wedge b$ et où u et v sont les coefficients en question.

Mise en pratique pour $(390; 525)$:

525	1	0
390	0	1
135	1	-1
120	-2	3
15	3	-4
0	-26	35

Et donc $\text{PGCD}(390; 525) = 15$ et $u = 3$ et $v = -4$.

Exemple 9

Déterminer $(x; y) \in \mathbb{N}^2$ tels que : $x^2 - y^2 = 5440$ et $\text{PGCD}(x; y) = 8$.

Corrigé

$x \wedge y = 8 \Rightarrow \exists a, b \in \mathbb{N}$ tels que $x = 8a$, $y = 8b$ et $a \wedge b = 1$. Alors on a : $a^2 - b^2 = 85$ et $a \wedge b = 1$.

Or $a^2 - b^2 = 85 \Leftrightarrow (a - b)(a + b) = 85$ et comme $85 = 1 \times 85 = 5 \times 17$ et que $0 < a - b < a + b$

alors on est conduit aux deux systèmes $\begin{cases} a - b = 1 \\ a + b = 85 \end{cases}$ et $\begin{cases} a - b = 5 \\ a + b = 17 \end{cases}$ qui donnent les solutions :

$(a; b) = (11; 6), (43; 42)$. D'où, en multipliant ces solutions par 8, on obtient les solutions recherchées $(x; y) = (88; 48), (344; 336)$.

VII. Système de numération à base b

Théorème 1 et définition :

Soit b un entier naturel autre que 0 et 1.

Pour tout entier naturel N , il existe un entier naturel non nul n et $n+1$ entiers $a_0, a_1, \dots, a_n$ tels que :

$$N = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0$$

avec $0 < a_n < b$ et $\forall k \in \llbracket 1, n-1 \rrbracket, 0 \leq a_k < b$

On dit que l'entier N s'écrit $a_n a_{n-1} \dots a_1 a_0$ dans le système de numération à base b .

S'il y a possibilité de confusion, on écrit parfois : $N = \overline{a_n a_{n-1} \dots a_1 a_0}_b$.

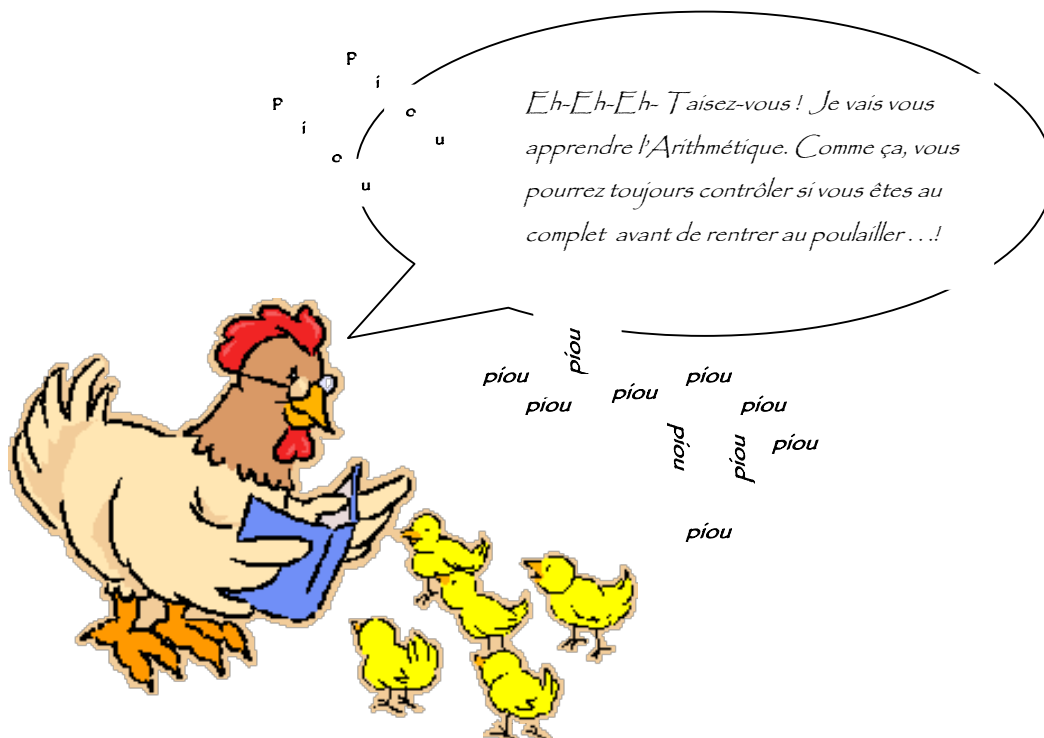
- ✓ Si $b = 10$, on parle de système décimal et on utilise les dix chiffres usuels : 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9.
- ✓ Si $b > 10$, On complète la liste des dix chiffres usuels par des lettres de l'alphabet. Ainsi, à titre d'exemple, le système à base « douze » (système duodécimal) utilise les chiffres 0, 1, 2, 3, 4 ; 5, 6, 7, 8, 9, A, B, où A désigne « le chiffre dix » et B représente « le chiffre onze ».

Exemples :

En base 6 : $\overline{2035} = 2 \times 6^3 + 0 \times 6^2 + 3 \times 6 + 5$ (= 455 en base 10)

En base 12 : $\overline{85A2B} = 8 \times 12^4 + 5 \times 12^3 + \underbrace{10}_A \times 12^2 + 2 \times 12 + \underbrace{11}_B$ (= 176 003 en base 10)

En base 2 : $\overline{10011011} = 1 \times 2^7 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2 + 1$ (= 155 en base 10)



Exemples d'application

Exemple 11

Écrire 475 en base 7.

Corrigé

On effectue les divisions successives :

• de 475 par 7 : $475 = 7 \times 67 + 6 \quad 0 \leq 6 < 7$

• de 67 par 7 : $67 = 7 \times 9 + 4 \quad 0 \leq 4 < 7$

• de 9 par 7 : $9 = 7 \times 1 + 2 \quad 0 \leq 2 < 7$

On arrête les divisions par 7, lorsque le quotient (ici 1) devient inférieur à la base 7. On a :

$$475 = 7 \times 67 + 6 = 7 \times [7 \times 9 + 4] + 6 = 7 \times [7 \times (7 \times 1 + 2) + 4] + 6$$

Et donc : $475 = \boxed{1} \times 7^3 + \boxed{2} \times 7^2 + \boxed{4} \times 7 + \boxed{6}$.

D'où : 475 s'écrit $\overline{1\,246}$ en base 7 (On lit : « 1, 2, 4, 6 »).

Disposition pratique :

$$\begin{array}{r} 475 \overline{) 7} \\ 55 \overline{) 67} 7 \\ 6 4 9 \overline{) 7} \\ 2 1 \end{array}$$

Donc : 475 s'écrit $\overline{1\,246}$ en base 7

Exemple 12

Déterminer les chiffres x et y tels que le nombre s'écrivant $\overline{x2y}$ en base 6 s'écrive $\overline{3x2}$ en base 5.

Donner ce nombre dans le système décimal.

Corrigé

Les données de l'exercice nous conduisent à l'égalité :

$$x \times 6^2 + 2 \times 6 + y = 3 \times 5^2 + x \times 5 + 2$$

$$\text{avec } 0 < x < 5 \text{ et } 0 \leq y < 6$$

Cela nous donne $36x + 12 + y = 36 + 5x + 2$ soit $y = 65 - 31x$.

La condition $0 \leq y < 6$ s'écrit alors $0 \leq 65 - 31x < 6$; ce qui donne l'encadrement $\frac{59}{31} < x \leq \frac{65}{31}$ et

comme x est un entier alors la seule valeur acceptable est $x = 2$.

En remplaçant y par sa valeur $65 - 31x$ avec $x = 2$, on trouve $y = 3$.

Dans le système décimal, le nombre cherché est :

$$N = 3 \times 5^2 + 2 \times 5 + 2 = 87.$$



EXERCICES CORRIGES

Les méthodes sont les habitudes de l'esprit et les économies de la mémoire.

Rivaroll

Exercice 1

On n'est pas orphelin d'avoir perdu père et mère, mais d'avoir perdu l'espoir.

Vérifier que les entiers suivants sont des multiples de 37 :

1. Les nombres constitués de trois chiffres identiques (comme 222, 888, ...)
2. Les nombres constitués de six chiffres identiques (comme 555555, 999999, ...)
3. Les nombres de six chiffres obtenus en juxtaposant trois fois deux chiffres identiques (comme 717171, ...).

Corrigé

1. Les nombres constitués de trois chiffres identiques:

222, 333, ..., 999 sont tous divisibles par 111 et $111 = 3 \times 37$.

2. Les nombres constitués de six chiffres identiques :

$$111111 = 111000 + 111 = 111(1000 + 1) = 111 \times 1001$$

Donc le nombre 111111 est divisible par 111 donc par 37.

222222, 333333, 444444, ..., 999999 sont tous divisibles par 111111 donc par 111 et donc par 37.

3. Les nombres de six chiffres obtenus en juxtaposant trois fois deux chiffres identiques:

$$717171 = 710000 + 7100 + 71 = 71(10000 + 100 + 1) = 71 \times 10101$$

Or $10101 = 37 \times 273$, d'où 717171 est divisible par 37 car 10101 l'est.

Soit a et b deux chiffres.

$$\begin{aligned} ababab &= a \times 10^5 + b \times 10^4 + a \times 10^3 + b \times 10^2 + a \times 10 + b \\ &= (a \times 10 + b) 10^4 + (a \times 10 + b) \times 10^2 + (a \times 10 + b) \\ &= (a \times 10 + b) (10^4 + 10^2 + 1) = (a \times 10 + b) \times 10101. \end{aligned}$$

$ababab$ est donc divisible par 10101 donc divisible par 37.

Exercice 2

Si la barbe suffisait à la sagesse, un bouc vaudrait Platon.

1. Démontrer que le produit de deux entiers naturels consécutifs est pair.

2. Le produit de trois entiers naturels consécutifs est-il : a) pair ? b) un multiple de 3 ? c) Un multiple de 6 ?

Corrigé

1. Démontrer que le produit de deux entiers consécutifs est pair :

Le produit de deux entiers naturels consécutifs est de la forme $n(n+1)$.

Deux cas se présentent alors.

➤ n est pair

Alors 2 divise n donc 2 divise $n \times (n+1)$

➤ n est impair

Alors $n+1$ est pair donc 2 divise $n+1$ donc 2 divise $n \times (n+1)$.

2. Le produit de trois entiers naturels consécutifs est-il :

Le produit de trois entiers naturels consécutifs est de la forme $n(n+1)(n+2)$.

a) **pair ?** : On a vu que pour tout entier naturel n , 2 divise $n(n+1)$ donc 2 divise $n(n+1)(n+2)$.

Donc $n(n+1)(n+2)$ est pair

b) **un multiple de 3 ?**

On considère le reste de la division de n par 3. Trois cas se présentent

→ le reste de la division par 3 de n est 0

3 divise alors n donc 3 divise aussi $n(n+1)(n+2)$

→ le reste de la division de n par 3 est 1.

n s'écrit alors $3q + 1$ où q est un entier naturel. On a alors : $n + 2 = 3q + 1 + 2 = 3q + 3 = 3(q + 1)$
 3 divise donc $n + 2$ donc 3 divise $n(n + 1)(n + 2)$
 $\rightarrow$ le reste de la division de n par 3 est 2 .
 n s'écrit alors $3q + 2$ où q est un entier naturel. On a alors : $n + 1 = 3q + 2 + 1 = 3q + 3 = 3(q + 1)$
 3 divise donc $n + 1$ donc 3 divise $n(n + 1)(n + 2)$
c) Un multiple de 6 ?
 3 et 2 divisent $n(n + 1)(n + 2)$ et 3 et 2 sont premiers donc 3×2 divisent $n(n + 1)(n + 2)$.

Exercice 3	Il vaut mieux avoir l'œuf aujourd'hui que la poule demain.
-------------------	---

Parmi tous les entiers positifs multiples de 2004, quels sont ceux qui ont exactement 20 diviseurs positifs ?

Corrigé

Soit N un multiple positif de 2004, donc $N = k \times 2004 = k \times 2^2 \times 3^1 \times 167^1$.
Le nombre des diviseurs positifs de 2004 est $(2 + 1) \times (1 + 1) \times (1 + 1) = 12$.
Donc si $k > 1$ alors k contiendra au moins un nombre premier et donc le nombre des diviseurs positifs de N est au moins $12 \times (1 + 1) = 24$. Par suite pour que N soit une solution du problème alors k doit être égal à 1 et N doit être de la forme $2^{(2+a)} \times 3^{(1+b)} \times 167^{(1+c)}$ avec a, b et c trois entiers naturels.
Dans ce cas le nombre de diviseurs de N est $d(N) = (2 + a + 1) \times (1 + b + 1) \times (1 + c + 1)$, c'est à dire $d(N) = (3 + a) \times (2 + b) \times (2 + c)$.
Or on veut que $d(N) = 20 = 5 \times 2^2$ alors il faut que $a = 2, b = 0$ et $c = 0$.
Conclusion : $N = 2^4 \times 3^1 \times 167^1 = 8016$.

Exercice 4	C'est avec l'eau du corps que l'on tire l'eau du puits.
-------------------	--

On divise 2003 par un entier n , le reste est égal à 8. On divise alors 3002 par n , le reste obtenu est 27. Que vaut n ?

Corrigé

On a : $\begin{cases} 2003 = an + 8 \\ 3002 = bn + 27 \end{cases} \Leftrightarrow \begin{cases} 1995 = an \\ 2975 = bn \end{cases}$
Ainsi n divise 1995 et 2975 et donc divise aussi $1995 \wedge 2975$.
Déterminons $d = 1995 \wedge 2975$ par l'algorithme d'Euclide :
On a : $2975 = 1995 \times 1 + 980$
 $1995 = 980 \times 2 + 35$
 $980 = 35 \times 28 + 0$.
Donc $d = 1995 \wedge 2975 = 35$ et comme les restes doivent être inférieurs à n , on en déduit que $n \geq 28$ et donc on peut conclure que $n = 35$.

Exercice 5	L'esprit est comme un parachute... il fonctionne mieux quand il est ouvert.
-------------------	--

Quelles sont toutes les listes d'entiers naturels consécutifs dont la somme vaut 2005 ?

Corrigé

Désignons par n un entier naturel et k un entier naturel non nul donc les nombres suivants : $n, (n + 1), (n + 2), (n + 3), \dots$ et $(n + k)$ sont les entiers consécutifs cherchés.

On a :

$$n + (n + 1) + (n + 2) + (n + 3) + \dots + (n + k) = 2005 \Leftrightarrow (k + 1)n + ((k(k + 1))/2) = 2005$$

$$\Leftrightarrow 2(k + 1)n + k(k + 1) = 4010 \Leftrightarrow (k + 1)(2n + k) = 4010 = 2 \times 5 \times 401$$

Premier cas $n = 0$

On a alors $(k + 1)(0 + k) = 2 \times 5 \times 401$, ce qui est impossible car 4010 ne peut pas être le produit de deux facteurs consécutifs.

Deuxième cas $n > 0$

Donc $2n + k > k + 1$ et par suite :

$$(k + 1)(2n + k) = 2 \times 5 \times 401 \Leftrightarrow (k + 1, 2n + k) \in \{(2, 2005), (5, 802), (10, 401)\}$$

$$\Leftrightarrow (k, n) \in \{(1, 1002), (4, 399), (9, 196)\}$$

Conclusion: les listes solutions du problème :

- 1002 et 1003
- 399, 400, 401, 402 et 403
- 196, 197, 198, ..., 205

Exercice 6	La prudence a plus de part aux succès que la force.
-------------------	--

1. Montrer que le reste dans la division euclidienne du carré d'un entier par 4 est soit 0, soit 1.
2. Montrer que le nombre $R_n = \underbrace{111 \dots 111}_{n \text{ chiffres "1"}}$ n'est pas un carré si $n \geq 2$.

Les nombres R_n sont appelés repunits.

Corrigé

1. On sait que tout entier m s'écrit $m = 2k$ (m pair) ou bien $m = 2k + 1$ (m impair). On a donc :

→ Si $m = 2k$, $m^2 = 4k^2$ est un multiple de 4, il est de la forme 4ℓ .

→ Si $m = 2k + 1$, $m^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ est de la forme $4\ell + 1$.

Donc $\forall m \in \mathbb{N}$, on a : $m^2 \equiv 0 [4]$ ou bien $m^2 \equiv 1 [4]$.

2. On sait que, pour tout $n \geq 2$, on peut écrire :

$$R_n = \underbrace{111 \dots 111}_{n-2 \text{ chiffres "1"}} 11 = R_{n-2} \times 100 + 11 = R_{n-2} \times 4 \times 25 + 4 \times 2 + 3 = 4(25R_{n-2} + 2) + 3$$

et par suite : $R_n \equiv 3 [4]$ et donc, selon la question précédente, R_n ne peut pas être le carré d'un entier.

Exercice 7	Le fruit mûr tombe de lui même, mais il ne tombe pas dans la bouche.
-------------------	---

Le chiffre des unités du nombre naturel N est x . On effectue successivement les opérations suivantes :

- supprimer le chiffre des unités x du nombre N ;
- retrancher $2x$ du nombre obtenu.

Par exemple, le nombre 203 devient 20, puis 14.

Est-il toujours vrai que le nombre final est un multiple de 7 si et seulement si le nombre initial est un multiple de 7 ?

Corrigé

Posons $N = 10d + x$ avec x le chiffre des unités.

L'opération est :

$$\frac{N - x}{10} - 2x = d - 2x$$

Si l'idée est vraie le problème revient à montrer que : 7 divise $(10d + x) \Leftrightarrow 7$ divise $(d - 2x)$

En effet : $2(10d + x) + (d - 2x) = 7(3d)$

Par suite : 7 divise $(10d + x) \Rightarrow 7$ divise $7(3d) - 2(10d - x) = d - 2x$

7 divise $(d - 2x) \Rightarrow 7$ divise $7(3d) - (d - 2x) = 2(10d + x)$

$\Rightarrow 7$ divise $(10d - x)$ car 7 et 2 sont premiers entre eux.

Exercice 8	Si on te donne de la canne à sucre, ne demande pas à être payé pour la manger
-------------------	--

(Étude de produit de facteurs dans une factorielle)

Soit $n \in \mathbb{N}$ non premier et tel que $n \geq 6$. L'objectif de l'exercice est de montrer que : $n \mid (n - 2)!$.

1. Justifier qu'il existe deux entiers naturels a et b tels que :

$$n = ab \text{ et } a \geq 2 \text{ et } b \geq 2$$

2. Montrer que : $a \leq \frac{n}{2}$ et $b \leq \frac{n}{2}$ puis que $a \leq n - 2$ et $b \leq n - 2$.

3. On suppose que $a \neq b$.

Montrer que $n \mid (n - 2)!$

4. On suppose que $a = b$.

a. Justifier que $a \geq 3$.

b. Montrer que $1 \leq 2a \leq n - 2$.

c. Montrer que $n \mid (n - 2)!$

5. Conclure.

Corrigé

1. Puisque n n'est pas premier, il existe $(a, b) \in \mathbb{N} \times \mathbb{N}$ tel que :

$$n = ab, \quad 1 < a < n, \quad 1 < b < n.$$

On a alors : $a \geq 2$ et $b \geq 2$.

2. Comme $n = ab$ avec $a \geq 2$ et $b \geq 2$ alors $a = \frac{n}{b} \leq \frac{n}{2}$ et de même $b = \frac{n}{a} \leq \frac{n}{2}$.

D'autre part, on a :

$$\frac{n}{2} \leq n - 2 \Leftrightarrow n \leq 2n - 4 \Leftrightarrow n \geq 4$$

Donc dès que $n \geq 4$ (ici $n \geq 6$), on a : $\frac{n}{2} \leq n - 2$ et par suite : $a \leq n - 2$ et $b \leq n - 2$.

3. On suppose que $a \neq b$.

Dans ce cas, comme a et b sont distincts et inférieurs à $n - 2$ alors $ab = n$ divise $(n - 2)!$.

4. On suppose que $a = b$.

a. Si $a = b$ alors $n = ab = a^2$, et comme $n \geq 6$, on a $a^2 \geq 6$. Ce qui donne $a \geq 3$ car a est un entier.

b. On a, sans oublier à chaque passage que a est un entier naturel :

$$a \geq 3 \Leftrightarrow a - 1 \geq 2 \Leftrightarrow (a - 1)^2 \geq 4 \Leftrightarrow (a - 1)^2 \geq 3 \Leftrightarrow a^2 - 2a - 2 \geq 0 \Leftrightarrow a^2 - 2 \geq 2a$$

Or, $a^2 - 2 = n - 2$; d'où : $2a \leq n - 2$. Donc enfin : $1 \leq 2a \leq n - 2$.

c. Les entiers a et $2a$ sont distincts et inférieurs à $n - 2$, donc leur produit $a(2a) = 2a^2 = 2n$ divise l'entier $(n - 2)!$. Et comme n divise $2n$ alors $n \mid (n - 2)!$.

5. En conjuguant les résultats des questions 3 et 4, on peut conclure que $n \mid (n - 2)!$ pour tout naturel n non premier et supérieur à 6.

Exercice 9

Rien ne vient sans peine, sauf la pauvreté ou la mauvaise réputation.

Trois entiers a , b et c vérifient $a^2 = b^2 + c^2$

1.a. Montrer que l'un au moins des entiers a , b et c est pair;

b. Montrer que l'un au moins des entiers b et c est multiple de 3 ;

c. Montrer que l'un au moins des entiers a , b et c est multiple de 5.

d. Montrer que l'un au moins des entiers a , b et c est multiple de 4.

2. Montrer que si les entiers a , b et c vérifient $a^2 = b^2 + c^2$ alors 60 divise le produit abc .

Corrigé

1. La démarche adoptée dans cette première question consiste à étudier la congruence du carré d'un entier en modulo 3, 5, 4 et 8.

a. Raisonnons par l'absurde : supposons qu'aucun des entiers a , b et c n'est pair.

On sait qu'un entier et son carré ont même parité. Donc b et c sont impairs alors b^2 et c^2 sont impairs. La somme de deux impairs étant paire alors $a^2 = b^2 + c^2$ est pair et par suite a est pair. Ce qui est contradictoire à l'hypothèse. Donc au moins l'un des entiers a , b et c est pair.

b. Soit x un entier. Étudions x^2 en modulo 3 :

$x \equiv \dots [3]$	0	1	2
$x^2 \equiv \dots [3]$	0	1	1

Donc, en modulo 3, le carré d'un entier est congru soit à 0, soit à 1.

Supposons qu'aucun des deux entiers b et c n'est un multiple de 3. Dans ce cas, on a :

$$b^2 \equiv 1 [3] \quad \text{et} \quad c^2 \equiv 1 [3]$$

Et par suite : $a^2 \equiv 2 [3]$, ce qui est impossible.

Donc l'un au moins des entiers b et c est un multiple de 3.

c. Congruences de x^2 modulo 5 :

$x \equiv \dots [5]$	0	1	2	3	4
$x^2 \equiv \dots [5]$	0	1	4	4	1

Donc, en modulo 5, le carré d'un entier est congru à 0, à 1 ou à 4.

Supposons qu'aucun des trois entiers a , b et c n'est un multiple de 5. Dans ce cas, on sait qu'on a bien :

$$b^2 + c^2 \equiv 1 + 1 = 2 [5] \quad \text{ou} \quad b^2 + c^2 \equiv 1 + 4 \equiv 0 [5] \quad \text{ou} \quad b^2 + c^2 \equiv 4 + 4 \equiv 3 [5]$$

Or le cas $b^2 + c^2 \equiv 1 + 4 \equiv 0 [5]$ qui signifie $a^2 \equiv 0 [5]$ est écarté car a n'est pas multiple de 5 par hypothèse. Les deux autres cas donnent $a^2 \equiv 2 [5]$ ou $a^2 \equiv 3 [5]$; ce qui est impossible d'après le tableau de congruences. Donc l'un au moins des entiers a , b et c est un multiple de 5.

d. On distingue deux cas :

→ Si a , b et c sont tous pairs alors les entiers $a' = \frac{a}{2}$, $b' = \frac{b}{2}$ et $c' = \frac{c}{2}$ vérifient $a'^2 = b'^2 + c'^2$. Donc selon la question a, l'un au moins des entiers a' , b' et c' est pair et par suite l'un au moins des entiers a , b et c est divisible par 4.

→ Si un seul des trois entiers a , b et c est pair :

- si l'entier b est pair alors $b^2 = a^2 - c^2$ avec a et c impairs. Or on sait qu'en modulo 8, pour un entier impair $x = 2k + 1$ on a $x^2 = 4 \underbrace{k(k+1)}_{\text{pair}} + 1 \equiv 1 [8]$ et donc par différence, on a :

$b^2 \equiv 0 [8]$ et par suite $b \equiv 0 [4]$ (car $b \equiv 2 [4]$ entraînerait $b \equiv 4 [8]$). Donc 4 divise b .

- Si a est pair et donc b et c impairs alors comme en modulo 4, on a :

$$\text{pair}^2 \equiv 0 [4] \quad \text{et} \quad \text{impair}^2 \equiv 1 [4]$$

alors $a^2 \equiv 2 [4]$, ce qui est impossible. Donc un tel triplet pythagoricien n'existe pas.

Donc enfin l'un au moins des entiers a , b et c est un multiple de 4.

2. D'après la question 1, si trois entiers vérifient la relation pythagoricienne $a^2 = b^2 + c^2$ alors parmi les entiers a , b et c , il y a un multiple de 3, un multiple de 4 et un multiple de 5. Les entiers 3, 4 et 5 étant premiers entre eux deux à deux alors $3 \times 4 \times 5 = 60$ divise le produit $a \times b \times c$.

Exercice 10

Tout âge porte ses fruits, il faut savoir les cueillir.

(Nombres premiers jumeaux)

Deux nombres premiers sont dits « jumeaux » s'ils diffèrent de deux unités : 11 et 13 sont des jumeaux.

1. Donner au moins trois autres exemples de nombres jumeaux.
2. Si le couple $(n, n + 2)$ est constitué de nombres premiers jumeaux, montrer que nécessairement n a pour reste 2 dans la division euclidienne par 3.
3. Montrer que, toujours dans ce cas, $n + 4$ est nécessairement divisible par 3.
4. Quels sont alors les diviseurs de $n^2 + 2n$?

Corrigé

1. $(3, 5)$; $(5, 7)$; $(17, 19)$.

2. Soit $(n, n + 2)$ un couple de nombres premiers jumeaux.

Si $n \equiv 0 [3]$ alors n n'est pas premier ;

Si $n \equiv 1 [3]$ alors $n + 2 \equiv 0 [3]$ et donc $n + 2$ n'est pas premier ;

Donc la seule possibilité est $n \equiv 2 [3]$.

3. Si $n \equiv 2 [3]$ alors $n + 4 \equiv 6 [3]$ et comme $6 \equiv 0 [3]$, on a : $n + 4 \equiv 0 [3]$. Donc 3 divise $n + 4$.

4. Comme n et $n + 2$ sont tous deux premiers alors les seuls diviseurs de $n^2 + 2n = n(n + 2)$ dans $\mathbb{N}$ sont 1, n , $n + 2$ et $n^2 + 2n$.

Exercice 11

Pourquoi te servir de poison, si tu peux tuer avec du miel.

a , b , p et q sont des entiers relatifs tels que : $a = 9p + 4q$ et $b = 2p + q$.

Démontrer que : $\text{PGCD}(a ; b) = \text{PGCD}(p ; q)$.

Corrigé

Soit d un diviseur commun de a et de b . On sait que d divise toute combinaison linéaire à coefficients entiers de a et de b , donc d divise en particulier $a - 4b = (9p + 4q) - 4(2p + q)$, c'est-à-dire d divise p . De même, on démontre que d divise q .

Ainsi tout diviseur de a et b est un diviseur de p et q . Réciproquement, soit d' un diviseur de p et q . Alors d' divise les deux combinaisons entières $9p + 4q$ et $2p + q$ donc d' divise a et b .

L'ensemble des diviseurs de a et b est donc égal à l'ensemble des diviseurs de p et q , d'où :

$$\text{PGCD}(a, b) = \text{PGCD}(p, q).$$

Exercice 12

On ne peut pas rassasier un chameau en le nourrissant à la cuillère.

Quelles sont les valeurs possibles du PGCD de $9p + 4$ et $2p - 1$?

Donner les valeurs possibles de p dans le cas où $\text{PGCD}(9p + 4, 2p - 1) = 17$.

Corrigé

Soit d un diviseur de $9p + 4$ et $2p - 1$. L'entier d divise alors $2(9p + 4) - 9(2p - 1)$ et donc d divise 17.
Les valeurs possibles du PGCD de $9p + 4$ et $2p - 1$ sont donc 1 et 17.

$$\text{PGCD}(9p + 4, 2p - 1) = 17 \Leftrightarrow (S) \begin{cases} 9p + 4 \equiv 0 [17] \\ 2p - 1 \equiv 0 [17] \end{cases}$$

Si p est solution de (S) alors $(9p + 4) - 4(2p - 1) \equiv 0 [17]$ soit $p \equiv 9 [17]$.

Réciproquement, si $p = 9 + 17k$ alors $9p + 4 = 17(9k + 5)$ soit $9p + 4 \equiv 0 [17]$.

De même, on démontre que $2p - 1 = 17(2k + 1)$ Soit : $2p - 1 \equiv 0 [17]$. Donc p est solution de (S).

D'où 17 est le PGCD de $9p + 4$ et $2p - 1$ si et seulement si p s'écrit $17k + 9$, où k est un entier relatif.

Exercice 13

Le seul endroit où la réussite vient avant le travail, c'est dans le dictionnaire.

Soient a et b deux nombres entiers relatifs premiers entre eux. Le but de l'exercice est de montrer de trois manières différentes que ab et $a + b$ sont premiers entre eux.

1. Première démonstration.

a. Démontrer le lemme d'Euclide : « si l'entier premier p divise ab alors p divise a ou p divise b ».

b. En déduire que ab et $a + b$ sont premiers entre eux.

2. Deuxième démonstration.

a. Montrer que a et $a + b$ sont premiers entre eux. Que peut-on dire des entiers b et $a + b$?

b. Montrer que si trois entiers A , B et C sont tels que $\text{PGCD}(A; B) = 1$ et $\text{PGCD}(A; C) = 1$ alors

$$\text{PGCD}(A; B \times C) = 1.$$

c. Utiliser les questions 2.a et 2.b pour conclure que ab et $a + b$ sont premiers entre eux.

3. Troisième démonstration.

Les entiers a et b étant premiers entre eux, il existe, selon Bézout, deux entiers relatifs u et v (coefficients de Bézout) tels que $au + bv = 1$. On pose $S = a + b$ et $P = ab$.

Calculer $(au^2 + bv^2)S - (u - v)^2P$. En déduire que ab et $a + b$ sont premiers entre eux.

Corrigé

1. Première démonstration.

a. Soit p un nombre premier tel que p divise ab et p ne divise ni a , ni b .

On sait que : p divise $ab \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $kp = ab$. Donc : a / kp

Or a et p sont premiers entre, donc selon Gauss a / k . D'autre part : $a / k \Rightarrow \exists h \in \mathbb{Z}$ tel que $k = ah$.

En injectant la relation $k = ah$ dans l'égalité $kp = ab$, on obtient : $hp = b$.

Ce qui donne p divise b . Ce qui est contradictoire. En conclusion : si p divise ab alors p divise a ou p divise b .

b. Soit p un nombre premier qui divise ab et $a + b$.

Selon le lemme d'Euclide, p divise ab implique que p divise a ou p divise b .

Supposons que p divise a . Comme p divise $a + b$ alors p divise $(a + b) - a = b$ et par suite $p = 1$ car a et b sont premiers entre eux. Donc ab et $a + b$ sont premiers entre eux.

2. Deuxième démonstration.

a. Soit d un entier naturel qui divise a et $a + b$. On a :

$$\begin{aligned} \begin{cases} d/a \\ d/a + b \end{cases} &\Rightarrow d/(a + b) - a = b \\ &\Rightarrow \begin{cases} d/a \\ d/b \end{cases} \\ &\Rightarrow d = 1 \text{ car } a \text{ et } b \text{ sont premiers entre eux.} \end{aligned}$$

Donc a et $a + b$ sont premiers entre eux. On démontre de même que b et $a + b$ sont premiers entre eux.

b. On a :

$$\begin{aligned} \text{PGCD}(A; B) = 1 &\Leftrightarrow \exists u, v \in \mathbb{Z} \text{ tel que : } uA + vB = 1 \\ &\Rightarrow (uC)A + vBC = C \end{aligned}$$

Donc tout diviseur commun d de A et BC divise $(uC)A + vBC = C$, donc d divise $\text{PGCD}(A; C) = 1$.

D'où : $\text{PGCD}(A; B \times C) = 1$.

c. Comme $\text{PGCD}(a; b) = 1$ alors par application des résultats de la question 2.a, on déduit que :

$$\text{PGCD}(a + b; a) = 1 \text{ et } \text{PGCD}(a + b; b) = 1.$$

Selon 2.b, on peut conclure que : $\text{PGCD}(a + b ; ab) = 1$, donc ab et $a + b$ sont premiers entre eux.

3. Troisième démonstration.

Les entiers u et v sont tels que $ua + vb = 1$.

On a :

$$\begin{aligned}(au^2 + bv^2)S - (u - v)^2P &= (au^2 + bv^2)(a + b) - (u - v)^2ab \\ &= (au)^2 + (bv)^2 + abu^2 + abv^2 - (u^2 - 2uv + v^2)ab \\ &= (au)^2 + (bv)^2 + abu^2 + abv^2 - u^2ab + 2uvab - v^2ab \\ &= (au)^2 + 2uvab + (bv)^2 = (au + vb)^2 = 1^2 = 1\end{aligned}$$

Donc, selon le théorème de Bézout, les entiers $S = a + b$ et $P = ab$ sont premiers entre eux.

Exercice 14

Personne n'a jamais tout à fait tort. Même une horloge arrêtée donne l'heure juste deux fois par jour.

On considère les deux entiers $a = 5n + 1$ et $b = 3n - 3$ où $n \in \mathbb{N}^*$.

1. Montrer que tout diviseur commun de a et de b est un diviseur de 18.

2. Pour quelles valeurs de n a-t-on $a \wedge b = 9$?

3. Calculer n sachant que $a \wedge b = 9$ et $a \vee b = 1881$.

Corrigé

1. On a : $\begin{cases} d/a = 5n + 1 \\ d/b = 3n - 3 \end{cases} \Rightarrow d/3a - 5b = 18$.

Donc tout diviseur commun à a et b est un diviseur de 18.

2. On utilise la propriété : $a \wedge b = (a - kb) \wedge b = a \wedge (b - ka)$ pour k entier. Ainsi, on a :

$$\begin{aligned}a \wedge b &= (5n + 1) \wedge (3n - 3) = [(5n + 1) - (3n - 3)] \wedge (3n - 3) = (2n + 4) \wedge (3n - 3) \\ &= (2n + 4) \wedge [(3n - 3) - (2n + 4)] = (2n + 4) \wedge (n - 7) \\ &= [(2n + 4) - 2(n - 7)] \wedge (n - 7) = 18 \wedge (n - 7)\end{aligned}$$

Donc, on peut se permettre d'écrire :

$$\begin{aligned}a \wedge b = 9 &\Leftrightarrow 18 \wedge (n - 7) = 9 \Leftrightarrow 9/(n - 7) \text{ et } (n - 7) \wedge 2 = 1 \\ &\Leftrightarrow n - 7 = 9k \text{ et } 9k \wedge 2 = 1 \Leftrightarrow n - 7 = 9k \text{ et } k \text{ est impair} \\ &\Leftrightarrow n - 7 = 9(2\alpha + 1) \Leftrightarrow n = 18\alpha + 16 \text{ avec } \alpha \in \mathbb{N}.\end{aligned}$$

3. Si $a \wedge b = 9$ alors n est de la forme $18\alpha + 16$ et l'on a :

$$\begin{aligned}a &= 5n + 1 = 5(18\alpha + 16) + 1 = 90\alpha + 81 = 9(10\alpha + 9) \\ b &= 3n - 3 = 3(18\alpha + 16) - 3 = 54\alpha + 45 = 9(6\alpha + 5)\end{aligned}$$

Par suite, on peut écrire : $a \vee b = \frac{ab}{a \wedge b} = 9(10\alpha + 9)(6\alpha + 5)$

D'où : $a \vee b = 1881 \Leftrightarrow 9(10\alpha + 9)(6\alpha + 5) = 1881 \Leftrightarrow 60\alpha^2 + 104\alpha - 164 = 0$. L'équation du second degré $60\alpha^2 + 104\alpha - 164 = 0$ admet une solution évidente $\alpha = 1$, la 2^{ème} solution n'est pas entière.

Exercice 15

La persévérance, c'est ce qui rend l'impossible possible, le possible probable et le probable réalisé.

Montrer que pour tous entiers a et b , on a :

1. $\text{PGCD}(a^2 + b^2, ab) = [\text{PGCD}(a, b)]^2$;

2. $\text{PGCD}(a + b, \text{PPCM}(a, b)) = \text{PGCD}(a, b)$;

3. $\forall n \in \mathbb{N}^*, \text{PGCD}(a^n, b^n) = [\text{PGCD}(a, b)]^n$ et $\text{PPCM}(a^n, b^n) = [\text{PPCM}(a, b)]^n$. En déduire $\text{PGCD}(81, 144)$.

Corrigé

1. Posons $d = \text{PGCD}(a, b)$. Il existe $a', b' \in \mathbb{N}$ tels que $a = da'$ et $b = db'$ avec $\text{PGCD}(a', b') = 1$.

On a donc :

$$\begin{aligned}\text{PGCD}(a^2 + b^2, ab) &= \text{PGCD}((da')^2 + (db')^2, da'db') \\ &= \text{PGCD}(d^2(a'^2 + b'^2), d^2a'b') \\ &= d^2 \cdot \text{PGCD}(a'^2 + b'^2, a'b').\end{aligned}$$

Soit p un diviseur premier commun de $a'b'$ et $a'^2 + b'^2$. Alors p divise a' ou p divise b' .

Si p divise a' , alors p divise a'^2 et b'^2 donc p divise b' , ce qui est absurde car p serait diviseur commun à a' et b' , mais $\text{PGCD}(a', b') = 1$.

Si p divise b' , on obtient de même avec le même raisonnement.

On obtient finalement :

$$\text{PGCD}(a^2 + b^2, ab) = [\text{PGCD}(a, b)]^2$$

2. Soit $d = \text{PGCD}(a, b)$. Il existe $a', b' \in \mathbb{N}$ tels que $a = da'$ et $b = db'$ avec $\text{PGCD}(a', b') = 1$. Il existe deux entiers u et v tels que : $va + bu = d$.

En divisant par d , on a : $v(a' + b') + ua'b' = 1$.

Le théorème de Bézout implique que : $\text{PGCD}(a' + b', a'b') = 1$.

Calculons

$$\begin{aligned} \text{PGCD}(a + b, \text{PPCM}(a, b)) &= \text{PGCD}\left(d(a' + b'), \frac{da'db'}{\text{PGCD}(a, b)}\right) \\ &= \text{PGCD}(d(a' + b'), da'b') \\ &= d \times \text{PGCD}(a' + b', a'b') = d. \end{aligned}$$

3. Soit $d = \text{PGCD}(a, b)$, alors il existe 2 entiers a' et b' tels que :

$$a = da' \text{ et } b = db' \text{ avec } \text{PGCD}(a', b') = 1.$$

Il vient donc : $\text{PGCD}(a^n, b^n) = \text{PGCD}[(da')^n, (db')^n] = d^n \times \text{PGCD}(a'^n, b'^n)$.

Soit p un diviseur premier commun à a'^n et b'^n . Comme p divise a' et b' , alors p divise le nombre $\text{PGCD}(a', b') = 1$. D'où : $\text{PGCD}(a'^n, b'^n) = 1$.

Il vient ainsi : $\text{PGCD}(a^n, b^n) = d^n \times 1 = d^n = [\text{PGCD}(a, b)]^n$.

Maintenant calculons :

$$\text{PPCM}(a^n, b^n) = \frac{|a^n| \times |b^n|}{\text{PGCD}(a^n, b^n)} = \frac{(|a| \times |b|)^n}{[\text{PGCD}(a, b)]^n} = [\text{PPCM}(a, b)]^n$$

On a : $81 = 9^2$ et $144 = 12^2$, donc : $\text{PGCD}(81, 144) = [\text{PGCD}(9, 12)]^2 = 3^2 = 9$.

Exercice 16

Les proverbes ressemblent aux papillons ; on en attrape quelques-uns, les autres s'envolent.

1. Soit a, b et c des entiers non nuls avec $\text{PGCD}(a, b) = 1$. Montrer que : $\text{PGCD}(a, bc) = \text{PGCD}(a, c)$.

2. Si $\text{PGCD}(a, b) = 8$, à quoi est égal $\text{PGCD}(a^2, b^2)$?

3. Quelles sont les valeurs possibles de $\text{PGCD}(a^3, b^4)$?

Corrigé

1. Soit $d = \text{PGCD}(a, c)$. Il existe $a', c' \in \mathbb{Z}$ tels que $a = da'$, $c = dc'$ avec $\text{PGCD}(a', c') = 1$.

On a donc : $\text{PGCD}(a, bc) = \text{PGCD}(da', dbc') = d \times \text{PGCD}(a', bc')$.

On sait que $\text{PGCD}(a, b) = 1$ et $\text{PGCD}(a', c') = 1$. Donc il existe $r, s, u, v \in \mathbb{Z}$ tels que : $a'r + c's = 1$ et $ua + vb = 1$, ce qui entraîne en multipliant les deux identités membre à membre :

$$a'(aur + brv) + c'sua + c'svb = 1.$$

Et comme $a = da'$ alors $c'sua = c'suda'$ et par suite on peut écrire :

$$a'(aur + brv + c'sud) + sv(c'b) = 1.$$

D'après Bézout, on a : $\text{PGCD}(a', bc') = 1$.

Enfin : $\text{PGCD}(a, bc) = \text{PGCD}(da', dbc') = d \times \text{PGCD}(a', bc') = d = \text{PGCD}(a, c)$.

2. Si $\text{PGCD}(a, b) = 8$, alors selon l'exercice précédent : $\text{PGCD}(a^2, b^2) = [\text{PGCD}(a, b)]^2 = 8^2 = 64$.

3. Si $\text{PGCD}(a, b) = 8$, alors on peut écrire $a = 8\alpha$ et $b = 8\beta$ avec $\text{PGCD}(\alpha, \beta) = 1$.

Ainsi : $a^3 = 2^9 \alpha^3$ et $b^4 = 2^{12} \beta^4$, donc : $\text{PGCD}(a^3, b^4) = 2^9 \text{PGCD}(\alpha^3, 2^3 \beta^4)$.

Cherchons $\text{PGCD}(\alpha^3, 2^3 \beta^4)$. On peut décomposer $\alpha^3 = p_1^{3r_1} p_2^{3r_2} \dots p_n^{3r_n}$ et $\beta^4 = q_1^{3s_1} q_2^{3s_2} \dots q_m^{3s_m}$ où $\{p_1, \dots, p_n\} \cap \{q_1, \dots, q_m\} = \emptyset$ et $p_1 < p_2 < \dots < p_n$; $q_1 < q_2 < \dots < q_m$.

On a deux cas :

→ 1^{er} cas : si α est pair, alors $\alpha^3 = 2^{3r_1} p_2^{3r_2} \dots p_n^{3r_n}$

Dans ce cas, on a : $\text{PGCD}(\alpha^3, 2^3 \beta^4) = 2^3 \text{pgcd}(2^{3r_1} p_2^{3r_2} \dots p_n^{3r_n}, q_1^{3s_1} q_2^{3s_2} \dots q_m^{3s_m}) = 2^3$.

→ 2^{ème} cas : si α est impair, alors $\text{PGCD}(\alpha^3, 2^3 \beta^4) = 1$.

Finalement, on obtient : $\text{PGCD}(a^3, b^4) = \begin{cases} 2^{12} & \text{si } \alpha \text{ est pair} \\ 2^9 & \text{si } \alpha \text{ est impair} \end{cases}$

Exercice 17	Le volume d'une pizza de rayon z et d'épaisseur a est : $\pi z z a$
--------------------	---

Soit a, b et x trois entiers naturels non nuls et $d = a \wedge b$.

1. Montrer que $x \vee d$ divise $x \vee a$ et que $\frac{x \vee a}{x \vee d}$ divise $\frac{a}{d}$.

2. En déduire une autre relation analogue.

3.a. Montrer que :

$$\frac{x \vee a}{x \vee d} \wedge \frac{x \vee b}{x \vee d} = 1.$$

b. En déduire que : $x \vee (a \wedge b) = (x \vee a) \wedge (x \vee b)$.

Corrigé

1. * On sait que :

L'entier a est un multiple de d , donc tout multiple commun à x et a est un multiple commun à x et d et par suite $(x \vee d) \mid (x \vee a)$.

** On a également :

$$\begin{aligned} d/a &\Rightarrow xd / xa \\ &\Rightarrow xd \vee ad / xa \vee ad \\ &\Rightarrow d(x \vee a) / a(x \vee d) \\ &\Rightarrow \frac{a(x \vee d)}{d(x \vee a)} = k \text{ entier} \\ &\Rightarrow \frac{x \vee a}{x \vee d} = k \frac{a}{d} \\ &\Rightarrow \frac{x \vee a}{x \vee d} \text{ divise } \frac{a}{d} \end{aligned}$$

2. Les entiers a et b jouant des rôles symétriques, on peut donc remplacer a par b dans ce qui précède pour aboutir aux résultats analogues suivants :

$$(x \vee d) \text{ divise } (x \vee a) \text{ et } \frac{x \vee b}{x \vee d} \text{ divise } \frac{b}{d}.$$

3.a. D'après ce qui précède, on a :

$$\frac{x \vee a}{x \vee d} \text{ divise } \frac{a}{d} \text{ et } \frac{x \vee b}{x \vee d} \text{ divise } \frac{b}{d}$$

ce qui donne :

$$\frac{x \vee a}{x \vee d} \wedge \frac{x \vee b}{x \vee d} \text{ divise } \frac{a}{d} \wedge \frac{b}{d}.$$

Or, on sait que :

$$\frac{a}{d} \wedge \frac{b}{d} = \frac{a \wedge b}{d} = \frac{d}{d} = 1,$$

d'où :

$$\frac{x \vee a}{x \vee d} \wedge \frac{x \vee b}{x \vee d} = 1.$$

b. En multipliant l'égalité précédente par $x \vee d$, on obtient : $x \vee d = (x \vee a) \wedge (x \vee b)$ soit :

$$x \vee (a \wedge b) = (x \vee a) \wedge (x \vee b).$$

Exercice 18	Un homme doit être assez grand pour admettre ses erreurs, assez intelligent pour apprendre de celles-ci et assez fort pour les corriger.
--------------------	---

Soit a, b deux entiers naturels non nuls. On pose : $d = a \wedge b$ et $m = a \vee b$.

Soit x un entier naturel non nul.

1.a. Montrer que : $(x \wedge a)/(x \wedge m)$ et $(x \wedge b)/(x \wedge m)$.

b. Montrer que : $\left(\frac{x \wedge m}{x \wedge a}\right) / \frac{m}{a}$ et $\left(\frac{x \wedge m}{x \wedge b}\right) / \frac{m}{b}$.

2.a. Établir que :

$$\left(\frac{x \wedge m}{x \wedge a}\right) \wedge \left(\frac{x \wedge m}{x \wedge b}\right) = 1.$$

b. En déduire que : $x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b)$.

Corrigé

1.a. On sait que : $(x \wedge a)/a$ et a/m donc $(x \wedge a)/m$.

Comme $(x \wedge a)/x$ alors $(x \wedge a)/(x \wedge m)$. On démontre de même que : $(x \wedge b)/(x \wedge m)$.

b. Partant des relations de cours : $(x \wedge a) \times (x \vee a) = x \times a$ et $(x \wedge m) \times (x \vee m) = x \times m$, on peut déduire :

$$\frac{(x \wedge m)}{(x \wedge a)} \times \frac{(x \vee m)}{(x \vee a)} = \frac{x \times m}{x \times a} = \frac{m}{a}$$

Et par suite, on obtient :

$$\frac{(x \wedge m)}{(x \wedge a)} \text{ divise } \frac{m}{a}.$$

On démontre de manière analogue que :

$$\frac{(x \wedge m)}{(x \wedge b)} \text{ divise } \frac{m}{b}.$$

2.a. On pose : $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$.

Ainsi, on a : $\alpha \wedge \beta = 1$, $d \times m = a \times b$, $\frac{m}{a} = \frac{b}{d} = \beta$, $\frac{m}{b} = \frac{a}{d} = \alpha$

Donc :

$$\frac{m}{a} \wedge \frac{m}{b} = 1.$$

Comme, on a déjà établi, à la question précédente, que :

$$\frac{(x \wedge m)}{(x \wedge a)} \text{ divise } \frac{m}{a} \text{ et } \frac{(x \wedge m)}{(x \wedge b)} \text{ divise } \frac{m}{b}$$

alors, on conclut que :

$$\frac{(x \wedge m)}{(x \wedge a)} \wedge \frac{(x \wedge m)}{(x \wedge b)} \text{ divise } \frac{m}{a} \wedge \frac{m}{b} = 1$$

Et donc :

$$\left(\frac{x \wedge m}{x \wedge a} \right) \wedge \left(\frac{x \wedge m}{x \wedge b} \right) = 1.$$

b. Comme $\left(\frac{x \wedge m}{x \wedge a} \right)$ et $\left(\frac{x \wedge m}{x \wedge b} \right)$ sont premiers entre eux alors leur PPCM est leur produit c'est-à-dire :

$$\left(\frac{x \wedge m}{x \wedge a} \right) \vee \left(\frac{x \wedge m}{x \wedge b} \right) = \left(\frac{x \wedge m}{x \wedge a} \right) \times \left(\frac{x \wedge m}{x \wedge b} \right) = \frac{(x \wedge m)^2}{(x \wedge a)(x \wedge b)}.$$

Donc, on en déduit que :

$$(x \wedge m)^2 = (x \wedge a)(x \wedge b) \left[\left(\frac{x \wedge m}{x \wedge a} \right) \vee \left(\frac{x \wedge m}{x \wedge b} \right) \right] = \frac{(x \wedge a)(x \wedge b)(x \wedge m)}{x \wedge a} \vee \frac{(x \wedge a)(x \wedge b)(x \wedge m)}{x \wedge b}$$

Soit, après simplification :

$$(x \wedge m)^2 = (x \wedge b)(x \wedge m) \vee (x \wedge a)(x \wedge m) = (x \wedge m) \times [(x \wedge a) \vee (x \wedge b)]$$

ou plus simplement : $x \wedge m = (x \wedge a) \vee (x \wedge b)$.

Si l'on tient compte du fait que : $m = a \vee b$, cette dernière égalité peut être écrite sous la forme :

$$x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b).$$

Exercice 19

Notre entreprise dans la vie n'est pas de surpasser les autres, mais bien de se surpasser soi-même.

Soit n un entier naturel.

1.a. Déterminer, en fonction de la parité de n , du valeur du PGCD : $d = (n^2 + 1) \wedge (n + 1)$

b. Montrer que le nombre $n^2 + 1$ n'est pas un carré parfait pour tout entier n non nul.

2. Soit a , b et n trois entiers naturels non nuls tels que :

$$a \wedge b = 1 \text{ et } a(n^2 + 1) = b^2(n + 1).$$

a. Montrer que : $a \wedge b^2 = 1$ puis que : $a \leq n$ et $b \leq n$.

b. En déduire que : $(n^2 + 1) \wedge (n + 1) = 2$.

c. On pose $n^2 + 1 = 2p$ et $n + 1 = 2q$ avec $p \wedge q = 1$.

Montrer que : $q = a$ et $p = b^2$.

d. On suppose que : $b = a + 1$.

Calculer alors les entiers a , b et n .

Corrigé

1.a. Détermination de $(n^2 + 1) \wedge (n + 1)$:

$$\begin{aligned} \begin{cases} d/n^2 + 1 \\ d/n + 1 \end{cases} &\Rightarrow \begin{cases} d/(n+1)^2 - (n^2 + 1) \\ d/n + 1 \end{cases} \\ &\Rightarrow \begin{cases} d/2n \\ d/n + 1 \end{cases} \\ &\Rightarrow d/2(n+1) - 2n \\ &\Rightarrow d/2 \end{aligned}$$

Donc on a soit $d = 1$ ou $d = 2$.

Étudions les valeurs de d en fonction de la parité de n :

→ Si n est pair alors $n + 1$ et $n^2 + 1$ sont tous deux impairs et donc $d = 1$.

→ Si n est impair alors $n + 1$ et $n^2 + 1$ sont tous deux pairs et donc $d = 2$.

b. On sait que pour tout entier n non nul, on a : $n^2 < n^2 + 1 < (n + 1)^2$ et cela prouve sans équivoque que $n^2 + 1$ n'est pas un carré parfait.

2.a. * Montrons que : $a \wedge b^2 = 1$.

On rappelle la propriété : « Soit a, b et c trois entiers. Si $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases}$ alors $a \wedge (bc) = 1$ »

Comme, dans l'énoncé, on a donné : $a \wedge b = 1$ on peut appliquer cette propriété en prenant $b = c$ pour obtenir $a \wedge b^2 = 1$.

** Montrons que : $a \leq n$.

On a :

$$\begin{aligned} \begin{cases} a(n^2 + 1) = b^2(n + 1) \\ a \wedge b^2 = 1 \end{cases} &\Rightarrow \begin{cases} a / b^2(n + 1) \\ a \wedge b^2 = 1 \end{cases} \\ &\Rightarrow a/n + 1 \\ &\stackrel{\text{Gauss}}{\Rightarrow} a \leq n + 1 \end{aligned}$$

Si $a = n + 1$ alors on aurait $(n + 1)(n^2 + 1) = b^2(n + 1)$; l'entier $n + 1$ étant non nul, on peut déduire que : $n^2 + 1 = b^2$, c'est-à-dire que $n^2 + 1$ est un carré parfait. Ce qui n'est pas le cas. Donc $a \neq n + 1$ et par suite $a < n + 1$ autrement dit, a étant un entier, on a $a \leq n$.

*** Montrons que : $b \leq n$.

On a :

$$\begin{aligned} \begin{cases} a(n^2 + 1) = b^2(n + 1) \\ a \wedge b^2 = 1 \end{cases} &\Rightarrow \begin{cases} b^2 / a(n^2 + 1) \\ a \wedge b^2 = 1 \end{cases} \\ &\Rightarrow b^2/n^2 + 1 \\ &\stackrel{\text{Gauss}}{\Rightarrow} b^2 \leq n^2 + 1 \end{aligned}$$

Comme $n^2 + 1$ n'est pas un carré parfait alors $b^2 \neq n^2 + 1$ et par suite $b^2 \leq n^2$ soit $b \leq n$.

b. Montrons que : $(n^2 + 1) \wedge (n + 1) = 1$.

On sait d'après la question 1 qu'on a : $(n^2 + 1) \wedge (n + 1) = 1$ ou $(n^2 + 1) \wedge (n + 1) = 2$.

On suppose que : $(n^2 + 1) \wedge (n + 1) = 1$

L'égalité $a(n^2 + 1) = b^2(n + 1)$ implique que $n + 1 / a(n^2 + 1)$. Les entiers $n + 1$ et $n^2 + 1$ étant premiers entre eux, on peut conclure que : $n + 1 / a$. Ce qui est absurde car $a \leq n$.

Donc, on a : $(n^2 + 1) \wedge (n + 1) = 2$.

c. On pose $n^2 + 1 = 2p$ et $n + 1 = 2q$ avec $p \wedge q = 1$.

Dans ce cas, l'égalité $a(n^2 + 1) = b^2(n + 1)$ s'écrit $ap = b^2q$.

Alors, on a :

$$\begin{aligned} \textcircled{1} \quad &\begin{cases} ap = b^2q \\ a \wedge b^2 = 1 \end{cases} \stackrel{\text{Gauss}}{\Rightarrow} a/q \\ \textcircled{2} \quad &\begin{cases} ap = b^2q \\ a \wedge b^2 = 1 \end{cases} \stackrel{\text{Gauss}}{\Rightarrow} q/a \\ \textcircled{3} \quad &\begin{cases} ap = b^2q \\ a \wedge b^2 = 1 \end{cases} \stackrel{\text{Gauss}}{\Rightarrow} b^2/p \end{aligned}$$

On déduit de $\textcircled{1}$ et $\textcircled{2}$ (q et a étant des entiers naturels) que $q = a$. D'autre part, on a :

$$\textcircled{4} \left\{ \begin{array}{l} ap = b^2q \\ a \wedge b^2 = 1 \end{array} \right. \xRightarrow[\text{Gauss}]{} p/b^2$$

En combinant $\textcircled{3}$ et $\textcircled{4}$, on déduit que : $p = b^2$.

d. Si $b = a + 1$ alors $a \wedge b = 1$. D'après ce qui précède, on a : $n + 1 = 2a$ et $n^2 + 1 = 2b^2$.

En remplaçant $n + 1$ et $n^2 + 1$ par leurs valeurs dans l'identité : $(n + 1)^2 = n^2 + 2n + 1 = (n^2 + 1) + 2n$.

Soit : $4a^2 = 2b^2 + 2n = 2(a + 1)^2 + 2n = 2a^2 + 4a + 2 + 2n = 2a^2 + 4a + 2(n + 1) = 2a^2 + 4a + 4a$.

D'où : $a^2 - 4a = 0$. Comme $a \neq 0$, la seule valeur possible pour a est $a = 4$.

Pour $a = 4$, on a $b = a + 1 = 5$ et $n = 2a - 1 = 7$.

Exercice 20

La logique vous mènera de A à B. L'imagination vous mènera partout.

1. Soit a, b et c trois entiers naturels non nuls tels que : $a \wedge b = 1$ et $c^2 = a \times b$.

Montrer qu'il existe deux entiers naturels α et β tels que : $a = \alpha^2$ et $b = \beta^2$.

2. Soit x et y deux entiers naturels non nuls vérifiant : $x^2 = 2y^2 + 1$.

a. Déterminer le PGCD de x et y .

b. Déterminer le PGCD des deux entiers $x - 1$ et $x + 1$. (On remarquera que $(x - 1)(x + 1) = 2y^2$)

c. Démontrer que l'un des deux entiers $x - 1$ et $x + 1$ est pair, non divisible par 4.

d. On suppose que $x - 1$ est pair, non divisible par 4.

* Montrer que :

$$(x + 1) \wedge \left(\frac{x - 1}{2}\right) = 1.$$

** Montrer que les nombres $\sqrt{x + 1}$ et $\sqrt{\frac{x - 1}{2}}$ sont des entiers naturels qui divisent y .

Corrigé

1. On pose : $d = a \wedge c$. On sait qu'il existe deux entiers naturels α et β tels que :

$$a = \alpha d \text{ et } c = \beta d \text{ et } \alpha \wedge \beta = 1.$$

Alors, on a :

$$c^2 = a \times b \Leftrightarrow d^2 \beta^2 = b \alpha d \Leftrightarrow d \beta^2 = b \alpha.$$

On sait que : $\alpha \wedge \beta = 1 \Rightarrow \alpha \wedge \beta^2 = 1$, d'où :

$$\begin{aligned} d \beta^2 = b \alpha &\Rightarrow \beta^2 / b \alpha \\ &\xRightarrow[\text{Gauss}]{} \beta^2 / b \text{ car } \alpha \wedge \beta^2 = 1. \end{aligned}$$

Montrons ensuite que b / β^2 :

On a également : $d \beta^2 = b \alpha \Rightarrow b / d \beta^2$

Pour avoir le droit d'utiliser le théorème de Gauss afin de conclure que b / β^2 , il suffit que les entiers b et d soient premiers entre eux c'est-à-dire que $b \wedge d = 1$. Pour cela, on pose $\delta = b \wedge d$.

Donc, on peut écrire :

$$\begin{aligned} \begin{cases} \delta / b \\ \delta / d \end{cases} &\Rightarrow \begin{cases} \delta / b \\ \delta / \alpha d \end{cases} \\ &\Rightarrow \begin{cases} \delta / b \\ \delta / \alpha \end{cases} \text{ (car } \alpha d = a) \\ &\Rightarrow \delta / a \wedge b = 1 \\ &\Rightarrow \delta = 1 \end{aligned}$$

Donc les entiers b et d sont premiers entre eux et donc Gauss nous assure : $b / d \beta^2 \Rightarrow b / \beta^2$.

Enfin, on peut bien conclure que $b = \beta^2$.

D'autre part, en remplaçant b par β^2 dans l'égalité $d \beta^2 = b \alpha$, on obtient $\beta^2 \alpha = d \beta^2$ soit $\alpha = d$.

Comme $a = \alpha d$, on peut déduire que : $a = \alpha^2$ (CQFD). En conclusion : les entiers a et b sont deux carrés parfaits.

2.a. On a : $x^2 = 2y^2 + 1$ ou encore $x \times x + (-2y) \times y = 1$ et donc le théorème de Bézout nous autorise de dire que les entiers x et y sont premiers entre eux c'est-à-dire que $x \wedge y = 1$.

b. Détermination de $(x-1) \wedge (x+1)$:

On remarque que $(x+1) - (x-1) = 2$ pour en déduire que $x-1$ et $x+1$ sont de même parité. D'autre part, leur produit $(x-1) \times (x+1) = 2y^2$ étant pair, les entiers $x-1$ et $x+1$ sont tous deux pairs.

Posons : $\delta = (x-1) \wedge (x+1)$. On a :

$$\begin{cases} \delta / (x-1) \\ \delta / (x+1) \end{cases} \Rightarrow \delta / (x+1) - (x-1) = 2.$$

Donc : $\delta = 1$ ou $\delta = 2$. Mais les entiers $x-1$ et $x+1$ étant tous les deux pairs, leur PGCD ne peut pas être égal à 1. Donc, en conclusion : $(x-1) \wedge (x+1) = 2$.

c. Si les deux entiers $x-1$ et $x+1$ étaient tous deux divisibles par 4, leur PGCD ne pourrait pas être égal à 2.

2. Donc au moins l'un des deux entiers $x-1$ et $x+1$ n'est pas divisible par 4.

d. On suppose que $x-1$ est pair, non divisible par 4.

* Montrons que : $(x+1) \wedge \left(\frac{x-1}{2}\right) = 1$.

L'entier $x-1$ étant pair et non divisible par 4, il existe un entier σ tel que $x-1 = 4\sigma + 2$ soit encore $\frac{x-1}{2} = 2\sigma + 1$. Comme $x+1$ est pair, il existe un entier μ tel que $x+1 = 2\mu$.

On pose : $\nabla = (x+1) \wedge \left(\frac{x-1}{2}\right)$. (∇ se lit nabla)

Donc $\nabla = (2\mu) \wedge (2\sigma + 1)$. On remarque que ∇ est impair car $2\sigma + 1$ l'est.

On a :

$$\begin{cases} \nabla / (x+1) \\ \nabla / \left(\frac{x-1}{2}\right) \end{cases} \Rightarrow \begin{cases} \nabla / (x+1) \\ \nabla / (x-1) \end{cases} \Rightarrow \nabla / (x+1) \wedge (x-1) = 2$$

∇ étant un entier naturel impair qui divise 2, alors $\nabla = 1$ c'est-à-dire que $(x+1) \wedge \left(\frac{x-1}{2}\right) = 1$.

** Montrons que les nombres $\sqrt{x+1}$ et $\sqrt{\frac{x-1}{2}}$ sont des entiers naturels qui divisent y .

On a :

$$(x+1) \wedge \left(\frac{x-1}{2}\right) = 1 \quad \text{et} \quad (x+1) \times \left(\frac{x-1}{2}\right) = y.$$

Donc selon la 1^{ère} question, il existe deux entiers α et β tels que :

$$x+1 = \alpha^2 \quad \text{et} \quad \frac{x-1}{2} = \beta^2 \quad \text{avec} \quad y = \alpha\beta.$$

Donc les nombres $\sqrt{x+1} = \alpha$ et $\sqrt{\frac{x-1}{2}} = \beta$ sont des entiers naturels qui divisent y .

Exercice 21

Le succès, c'est vous aimer vous-même, c'est aimer ce que vous faites et c'est aimer comment vous le faites.

Une fraction $\frac{a}{b}$ est dite irréductible ou non simplifiable si les numérateur et dénominateur a et b sont des entiers premiers entre eux. Montrer que pour tout naturel non nul n , les fractions suivantes sont irréductibles :

$$f_1 = \frac{n}{kn+1} ; \quad f_2 = \frac{2n(4n^2+1)}{2n+1} ; \quad f_3 = \frac{15n^2+8n+6}{30n^2+21n+13}.$$

Corrigé

→ Pour $f_1 = \frac{n}{kn+1}$:

$$n \wedge (kn+1) = n \wedge (kn+1 - kn) = n \wedge 1 = 1 \Rightarrow f_1 \text{ est irréductible.}$$

→ Pour $f_2 = \frac{2n(4n^2+1)}{2n+1}$:

Il suffit de démontrer que $2n+1$ est premier avec chaque facteur du numérateur. En effet, $2n$ et $2n+1$ sont premiers entre eux car se sont deux entiers consécutifs.

$$D'autre part, on a : $2n \wedge (4n^2+1) = 2n \wedge (4n^2+1 - 2n \times 2n) = 2n \wedge 1 = 1$.$$

Donc f_2 est irréductible.

$$\rightarrow \text{Pour } f_3 = \frac{15n^2 + 8n + 6}{30n^2 + 21n} :$$

On calcule $(15n^2 + 8n + 6) \wedge (30n^2 + 21n + 13)$ par l'algorithme d'Euclide :

$$30n^2 + 21n + 13 = 2(15n^2 + 8n + 6) + 5n + 1$$

$$15n^2 + 8n + 6 = (3n + 1)(5n + 1) + 5$$

$$5n + 1 = n \times 5 + \boxed{1}$$

$$5 = 1 \times 5 + 0$$

Donc f_3 est irréductible.

Exercice 22

Étant donné que vous allez penser de toute façon, pensez donc Grand!

Trouver les entiers naturels n pour lesquels les fractions suivantes sont irréductibles :

$$f_1 = \frac{n+2}{n+15} \quad ; \quad f_2 = \frac{n^2+2n}{2n+3}.$$

Corrigé

$$\rightarrow \text{Pour } f_1 = \frac{n+2}{n+15} : f_1 = \frac{n+2}{n+15} \text{ irréductible} \Leftrightarrow (n+2) \wedge (n+15) = 1$$

$$\Leftrightarrow (n+2) \wedge (n+15-n-2) = 1$$

$$\Leftrightarrow (n+2) \wedge 13 = 1$$

$$\Leftrightarrow (n+2) \text{ n'est pas divisible par } 13$$

$$\Leftrightarrow n+2 \neq 13k, k \in \mathbb{N}^*$$

$$\Leftrightarrow n \neq 13k - 2, k \in \mathbb{N}^*$$

Donc la fraction $f_1 = \frac{n+2}{n+15}$ est irréductible si et seulement si n est un entier naturel qui ne s'écrit pas sous la forme $13k - 2$, (avec $k \in \mathbb{N}^*$).

$$\rightarrow \text{Pour } f_2 = \frac{n^2+2n}{2n+3} :$$

$$f_2 = \frac{n^2+2n}{2n+3} \text{ irréductible} \Leftrightarrow (n^2+2n) \wedge (2n+3) = 1$$

$$\Leftrightarrow n(n+2) \wedge (2n+3) = 1$$

$$\Leftrightarrow n \wedge (2n+3) = 1 \text{ et } (n+2) \wedge (2n+3) = 1$$

$$\text{Or, } (n+2) \wedge (2n+3) = (n+2) \wedge (|2n+3-2(n+2)|) = (n+2) \wedge 1 = 1, \forall n \in \mathbb{N}.$$

$$\text{D'autre part, on a : } n \wedge (2n+3) = n \wedge (2n+3-2 \times n) = n \wedge 3.$$

Ainsi, la fraction f_2 est irréductible si et seulement si $n \wedge 3 = 1$ autrement dit si n n'est pas multiple du nombre 3.

Exercice 23

J'ai plus peur d'une armée de 100 moutons menée par un lion qu'une armée de 100 lions menée par un mouton.

a, b et c étant trois entiers naturels, on considère la fraction :

$$F = \frac{an+b}{n-c} \quad (n > c).$$

1. Pour quelles valeurs de n , F est-elle un entier ?

2. A quels problèmes se ramène le calcul de la somme S de toutes les valeurs entières prises par la fraction F ?

Application : $a = 12, b = 96, c = 4$.

Corrigé

1. Par division euclidienne, on obtient :

$$F = a + \frac{b+ac}{n-c}.$$

Donc, F est un entier si, et seulement, si $n-c$ est un diviseur de $b+ac$, c'est-à-dire $n-c = d$ où d est un diviseur de $b+ac$, soit $n = c+d$.

2. Soit $d_1, d_2, \dots, d_p$ les diviseurs de $b+ac$ et soit d'_i le diviseur complémentaire de d_i , c'est-à-dire $d_i \times d'_i = b+ac$. Les valeurs entières de F sont données par :

$$F'_i = a + \frac{b+ac}{d_i} = a + d'_i \quad (\text{pour } i = 1, 2, \dots, p)$$

Donc, on a :

$$S = \sum_{i=1}^p F_i = \sum_{i=1}^p (a + d'_i) = ap + \sum_{i=1}^p d'_i = ap + \sum_{i=1}^p d_i \quad \text{car} \quad \sum_{i=1}^p d'_i = \sum_{i=1}^p d_i.$$

Donc le problème du calcul de la somme des valeurs entières prises par F se ramène à calculer :

→ Le nombre p des diviseurs de $b + ac$;

→ La somme des diviseurs de $b + ac$.

Application :

Pour $a = 12, b = 96, c = 4$, on a :

① $b + ac = 96 + 48 = 144 = 2^4 \times 3^2$ admet $p = 5 \times 3 = 15$ diviseurs dans $\mathbb{N}$.

$$\begin{aligned} \textcircled{2} S &= 12 \times 15 + \sum_{\substack{0 \leq i \leq 4 \\ 0 \leq j \leq 2}} 2^i \times 3^j = 180 + \left(\sum_{i=0}^4 2^i \right) \times \left(\sum_{j=0}^2 3^j \right) = 180 + \left(\frac{2^5 - 1}{2 - 1} \right) \left(\frac{3^3 - 1}{3 - 1} \right) = 583 \\ &\left(\sum_{\substack{0 \leq i \leq 4 \\ 0 \leq j \leq 2}} 2^i \times 3^j = \left(\sum_{i=0}^4 2^i \right) \times \left(\sum_{j=0}^2 3^j \right) \text{ car les indices } i \text{ et } j \text{ sont indépendants} \right) \end{aligned}$$

Exercice 24

Le succès, c'est se promener d'échecs en échecs tout en restant motivé.

Le PGCD de trois entiers

Soit a, b et c trois entiers relatifs.

Posons : $\text{PGCD}(a, b) = a \wedge b = \delta_1$; $\text{PGCD}(b, c) = b \wedge c = \delta_2$; $\text{PGCD}(c, a) = c \wedge a = \delta_3$.

1. Montrer que : $\delta_1 \wedge c = \delta_2 \wedge a = \delta_3 \wedge b$.

On vient de montrer que : $\text{PGCD}[\text{PGCD}(a, b), c] = \text{PGCD}[a, \text{PGCD}(b, c)]$. Cette valeur commune est appelée le PGCD des trois entiers a, b et c et se note $\text{PGCD}(a, b, c)$ ou encore $a \wedge b \wedge c$.

2. Application :

a. Déterminer le PGCD de 4 116, 28 420 et 33 810 (Pour réduire la complexité de l'algorithme d'Euclide, commencer d'abord à associer le plus grand nombre avec le plus petit).

b. Déterminer $p \in \mathbb{Z}, q \in \mathbb{Z}, r \in \mathbb{Z}$ tels que :

$$\text{PGCD}(4\,116, 28\,420, 33\,810) = p \cdot 4\,116 + q \cdot 28\,420 + r \cdot 33\,810.$$

Corrigé

1. Posons $d_1 = \delta_1 \wedge c$, $d_2 = \delta_2 \wedge a$ et $d_3 = \delta_3 \wedge b$.

Montrons que : $d_1 = d_2 = d_3$.

On a :

$$\begin{aligned} \begin{cases} d_1 / \delta_1 \\ d_1 / c \end{cases} &\Rightarrow \begin{cases} d_1 / a \\ d_1 / b \\ d_1 / c \end{cases} \\ \begin{cases} d_1 / a \\ d_1 / b \\ d_1 / c \end{cases} &\Rightarrow \begin{cases} d_1 / a \\ d_1 / \delta_2 \end{cases} \\ \begin{cases} d_1 / a \\ d_1 / \delta_2 \end{cases} &\Rightarrow d_1 / \delta_2 \wedge a = d_2 \\ d_1 / d_2 &\Rightarrow d_1 \leq d_2 \end{aligned}$$

On démontre de manière analogue que $d_2 \leq d_1$. Donc $d_1 = d_2$.

Dans l'écriture $\text{PGCD}(\alpha, \beta)$, l'ordre entre α et β étant peu importe, on peut conclure que $d_3 = d_1$.

On peut donc bien conclure que :

$$\text{PGCD}[\text{PGCD}(a, b), c] = \text{PGCD}[a, \text{PGCD}(b, c)] \text{ ou encore } (a \wedge b) \wedge c = a \wedge (b \wedge c).$$

2.a. A la lumière du résultat de la 1^{ère} question, on peut écrire :

$$\text{PGCD}(4\,116, 28\,420, 33\,810) = \text{PGCD}[(4\,116, 33\,810), 28\,420] = (4\,116 \wedge 33\,810) \wedge 28\,420$$

(On associe tout d'abord le plus grand nombre avec le plus petit)

Utilisons l'algorithme d'Euclide pour le PGCD(4 116, 33 810) :

$$\begin{aligned} 33\,810 &= 8 \times 4\,116 + 882 \\ 4\,116 &= 4 \times 882 + 588 \\ 882 &= 1 \times 588 + 294 \\ 588 &= 2 \times 294 + 0 \end{aligned}$$

Donc $\text{PGCD}(4\,116, 33\,810) = 294$.

Déterminons maintenant le PGCD(294, 28 420) :

$$\begin{aligned} 28\,420 &= 96 \times 294 + 196 \\ 294 &= 1 \times 196 + 98 \\ 196 &= 2 \times 98 + 0 \end{aligned}$$

Donc $\text{PGCD}(294, 28\,420) = 98$ et par suite $\text{PGCD}(4\,116, 28\,420, 33\,810) = 98$.

b. Détermination des coefficients p , q et r :

On exprime les restes successifs en fonction des trois nombres. On a :

$$\begin{aligned} 33\,810 &= 8 \times 4\,116 + \underline{882} \Rightarrow \underline{882} = -8 \times 4\,116 + 33\,810 \\ 4\,116 &= 4 \times 882 + \underline{588} \Rightarrow \underline{588} = 4\,116 - 4 \times 882 \\ &= 33 \times 4\,116 - 4 \times 33\,810 \\ 882 &= 1 \times 588 + \underline{294} \Rightarrow \underline{294} = 882 - 588 \\ &= -41 \times 4\,116 + 5 \times 33\,810 \end{aligned}$$

D'autre part :

$$\begin{aligned} 28\,420 &= 96 \times 294 + \underline{196} \Rightarrow \underline{196} = 28\,420 - 96 \times 294 \\ &= 3\,936 \times 4\,116 + 28\,420 - 480 \times 33\,810 \\ 294 &= 1 \times 196 + \underline{98} \Rightarrow \underline{98} = 294 - 196 \\ &= -3\,977 \times 4\,116 - 28\,420 + 485 \times 33\,810 \end{aligned}$$

Donc finalement, on trouve : $p = -3\,977$, $q = -1$, $r = 485$.

Exercice 25

Dans le domaine des idées, tout dépend de l'enthousiasme. Dans le monde réel, tout repose sur la persévérance.

Soit a , b et c trois entiers naturels tels que : $a \wedge b = 24$ et $b \wedge c = 36$.

1. Déterminer $a \wedge b \wedge c$.

2. Déterminer les entiers a , b et c sachant que : $a + b + c = 300$.

Corrigé

1. Détermination de $a \wedge b \wedge c$:

$$\begin{aligned} a \wedge b \wedge c &= a \wedge (b \wedge c) \text{ car } b \wedge b = b \\ a \wedge b \wedge c &= (a \wedge b) \wedge (b \wedge c) = 24 \wedge 36 = 12. \end{aligned}$$

2. Détermination des entiers a , b et c : Comme $a \wedge b \wedge c = 12$ alors il existe trois entiers non nuls a' , b' et c' tels que : $a = 12a'$, $b = 12b'$, $c = 12c'$.

Les égalités $a \wedge b = 24$ et $b \wedge c = 36$ peuvent donc s'écrire : $12a' \wedge 12b' = 24$ et $12b' \wedge 12c' = 36$ ou encore, après avoir simplifié par 12 : $a' \wedge b' = 2$ et $b' \wedge c' = 3$.

On peut déduire de ces deux dernières relations, prises conjointement, que :

- a' est un multiple et non de 3 ;
- b' est multiple de 2 et de 3 et donc b' est un multiple de 6 (Gauss) ;
- c' est un multiple de 3 et non de 2.

D'autre part, l'égalité $a + b + c = 300$ se transforme en l'égalité $a' + b' + c' = 25$.

On envisage plusieurs cas suivant les valeurs de a' :

$$\rightarrow a' = 2 \Rightarrow b' + c' = 23$$

- $\rightarrow b' = 6$ et $c' = 17$ (impossible car $c' = 17$ n'est pas un multiple de 3) ;
- $\rightarrow b' = 12$ et $c' = 11$ (impossible car $c' = 11$ n'est pas un multiple de 3) ;
- $\rightarrow b' = 18$ et $c' = 5$ (impossible car $c' = 5$ n'est pas un multiple de 3).

$$\rightarrow a' = 4 \Rightarrow b' + c' = 21$$

- $\rightarrow b' = 6$ et $c' = 15$;
- $\rightarrow b' = 12$ et $c' = 9$;
- $\rightarrow b' = 18$ et $c' = 3$.

- $\rightarrow a' = 8 \Rightarrow b' + c' = 17$
 $\rightarrow b' = 6$ et $c' = 11$ (impossible car $c' = 11$ n'est pas un multiple de 3);
 $\rightarrow b' = 12$ et $c' = 5$ (impossible car $c' = 5$ n'est pas un multiple de 3).
 $\rightarrow a' = 10 \Rightarrow b' + c' = 15$
 $\rightarrow b' = 6$ et $c' = 9$;
 $\rightarrow b' = 12$ et $c' = 3$.
 $\rightarrow a' = 14 \Rightarrow b' + c' = 11$
 $\rightarrow b' = 6$ et $c' = 5$ (impossible car $c' = 5$ n'est pas un multiple de 3).
 $\rightarrow a' = 16 \Rightarrow b' + c' = 9$
 $\rightarrow b' = 6$ et $c' = 3$.

Donc en récapitulant tous les cas, on peut dire que :

$$(a', b', c') \in \{(4, 6, 15), (4, 12, 9), (4, 18, 3), (10, 6, 9), (10, 12, 3), (16, 6, 3)\}.$$

Comme $(a, b, c) = (12a', 12b', 12c')$ alors l'ensemble des solutions est :

$$(S) = \{(48, 72, 180), (48, 144, 108), (48, 216, 36), (120, 72, 108), (120, 144, 36), (192, 72, 36)\}.$$

Exercice 26

**Les bonnes mathématiques, ce n'est pas le nombre de réponses que vous savez.
C'est la façon dont vous vous comportez lorsque vous ne savez pas.**

Soit p un entier naturel premier tel que $p \equiv 3 \pmod{4}$.

1.a. Montrer que l'équation : $x^2 + 1 \equiv 0 \pmod{p}$ n'admet pas de solution dans $\mathbb{Z}$.

b. En déduire que : $\forall (x, y) \in \mathbb{Z}^2, \left(p/x^2 + y^2 \Leftrightarrow \begin{cases} p/x \\ p/y \end{cases} \right)$

2.a. Montrer que l'équation $x^2 + y^2 = pz^2$ où $x \wedge y \wedge z = 1$ n'admet aucune solution dans $(\mathbb{N}^*)^3$.

b. Résoudre dans $\mathbb{Z}^3$ l'équation $x^2 + y^2 = pz^2$.

Corrigé

1.a. On suppose qu'il existe un entier relatif a solution de l'équation : $x^2 + 1 \equiv 0 \pmod{p}$. Ainsi, on a :

$$\begin{aligned}
 a^2 + 1 &\equiv 0 \pmod{p} \Leftrightarrow a^2 \equiv -1 \pmod{p} \\
 &\Rightarrow a^4 \equiv 1 \pmod{p}
 \end{aligned}$$

Comme $a^2 \equiv -1 \pmod{p}$ alors p ne divise pas a et le petit théorème de Fermat remplit donc les conditions de son application : $a^{p-1} \equiv 1 \pmod{p}$. Donc $p-1$ est un multiple de 4 c'est-à-dire que $p \equiv 1 \pmod{4}$, ce qui est contradictoire à l'hypothèse $p \equiv 3 \pmod{4}$.

En conclusion, l'équation $x^2 + 1 \equiv 0 \pmod{p}$ n'admet pas de solution dans $\mathbb{Z}$.

b. Soit x et y deux entiers relatifs. Il s'agit d'établir une équivalence qu'on scindera en deux implications réciproques :

$\Leftarrow$ Ce sens est trivial.

$$\text{Si } \begin{cases} p/x \\ p/y \end{cases} \text{ alors } \begin{cases} p/x^2 \\ p/y^2 \end{cases} \text{ et par suite } p/x^2 + y^2.$$

$\Rightarrow$ Supposons que $p/x^2 + y^2$ et montrons que $\begin{cases} p/x \\ p/y \end{cases}$

Tout d'abord, on ne peut que remarquer que :

$$p/x \Leftrightarrow p/x^2 \Leftrightarrow p/x^2 + y^2 - x^2 \Leftrightarrow p/y^2 \Leftrightarrow p/y$$

Donc il suffit de montrer seulement que p/x . Pour cela, nous procéderons par un raisonnement par l'absurde : on suppose que p ne divise pas x .

Comme p est premier ne divisant pas x alors $p \wedge x = 1$. Donc le théorème de Bézout assure l'existence de deux entiers relatifs α et β tels que : $\alpha p + \beta x = 1$.

On a :

$$\begin{aligned}
 \alpha p + \beta x &= 1 \Rightarrow \beta x \equiv 1 \pmod{p} \\
 &\Rightarrow \beta^2 x^2 \equiv 1 \pmod{p}
 \end{aligned}$$

Comme $p/x^2 + y^2$ c'est-à-dire $x^2 + y^2 \equiv 0 \pmod{p}$ soit en multipliant par β^2 : $\beta^2 x^2 + \beta^2 y^2 \equiv 0 \pmod{p}$ ou encore $1 + \beta^2 y^2 \equiv 0 \pmod{p}$ car $\beta^2 x^2 \equiv 1 \pmod{p}$.

$$1 + \beta^2 y^2 \equiv 0 \pmod{p} \Leftrightarrow (\beta y)^2 + 1 \equiv 0 \pmod{p}$$

Donc βy est solution de l'équation $x^2 + 1 \equiv 0 \pmod{p}$, ce qui est en contradiction avec le résultat de la première question. D'où p divise x et par suite p divise aussi y .

2.a. Montrons que l'équation $x^2 + y^2 = pz^2$ où $x \wedge y \wedge z = 1$ n'admet aucune solution dans $(\mathbb{N}^*)^3$.
Raisonnons par l'absurde en supposant que l'équation admet une solution (a, b, c) dans $(\mathbb{N}^*)^3$.
Donc (a, b, c) vérifie :

$$\begin{cases} a^2 + b^2 = pc^2 \\ a \wedge b \wedge c = 1 \end{cases}$$

On a :

$$\begin{aligned} a^2 + b^2 = pc^2 &\Rightarrow p \mid a^2 + b^2 \\ &\Rightarrow \begin{cases} p \mid a \\ p \mid b \end{cases} \text{ (selon question précédente)} \\ &\Rightarrow \exists k, k' \in \mathbb{N}^* \text{ tels que } \begin{cases} a = kp \\ b = k'p \end{cases} \end{aligned}$$

Donc, dans ce cas, on a également :

$$a^2 + b^2 = pc^2 \Leftrightarrow k^2p^2 + k'^2p^2 = pc^2 \Leftrightarrow p(k^2 + k'^2) = c^2$$

Et donc $p \mid c^2$, et vu que p est premier alors $p \mid c$. On déduit donc que p divise chacun des trois entiers a, b et c soit $p \mid a \wedge b \wedge c = 1$ et par suite $p = 1$. Ceci contredit la primalité de p .

En conclusion, l'équation $x^2 + y^2 = pz^2$ avec $x \wedge y \wedge z = 1$ n'admet pas de solution dans $(\mathbb{N}^*)^3$.

b. Résolvons dans $\mathbb{Z}^3$ l'équation $x^2 + y^2 = pz^2$.

Tout d'abord, on remarque que :

→ Le triplet $(0, 0, 0)$ est une solution triviale ;

→ Si (x, y, z) est une solution de l'équation $x^2 + y^2 = pz^2$ alors le triplet $(-x, -y, -z)$ en est une autre. Donc, il suffit de résoudre l'équation dans $(\mathbb{N}^*)^3$.

On suppose qu'il existe une solution (x, y, z) dans $(\mathbb{N}^*)^3$. On pose $d = x \wedge y \wedge z$ (on a $d \geq 1$).

On a :

$$\exists (x', y', z') \in (\mathbb{N}^*)^3 \text{ tel que } \begin{cases} x = dx' \\ y = dy' \\ z = dz' \\ x' \wedge y' \wedge z' = 1 \end{cases}$$

L'équation $x^2 + y^2 = pz^2$ requiert donc les relations suivantes :

$$\begin{cases} x'^2 + y'^2 = pz'^2 \\ (x', y', z') \in (\mathbb{N}^*)^3 \\ x' \wedge y' \wedge z' = 1 \end{cases}$$

Mais la question 2.a, ce dernier système n'admet de solution dans $(\mathbb{N}^*)^3$ et donc n'admet pas non plus de solution dans $(\mathbb{Z}^*)^3$. Enfin, on peut conclure que : $\mathcal{S} = \{(0, 0, 0)\}$.

Exercice 27

Un mathématicien est un aveugle qui, dans une pièce sombre, cherche un chat noir qui n'y est pas.

Déterminer le PGCD de tous les entiers de la forme $(a - b)(b - c)(c - d)(d - a)(b - d)(a - c)$ où les entiers a, b, c, d parcourent $\mathbb{Z}$.

Corrigé

Si on calcule le produit en question pour $a = 0, b = 1, c = 2, d = 3$, on trouve -12 , donc le PGCD en question divise nécessairement $12 = 3 \times 4$.

Réciproquement, nous allons montrer que ce PGCD est 12, en montrant que tous les nombres de cette forme sont divisibles par 3 et par 4.

Un entier n divise la différence entre deux des entiers a, b, c, d si ces entiers ont le même reste dans la division euclidienne par n . Puisqu'il n'y a que 3 restes possibles modulo 3, il y a forcément deux entiers parmi a, b, c, d qui ont le même reste. Tous les produits considérés dans l'énoncé sont donc divisibles par 3. Regardons maintenant les restes modulo 4 : il y a alors deux cas à considérer.

→ S'il existe deux entiers parmi a, b, c, d qui ont le même reste dans la division euclidienne par le nombre 4. La différence entre ces deux entiers sera divisible par 4.

→ Si a, b, c, d ont tous des restes différents modulo 4, cela veut dire que les 4 restes possibles dans la division euclidienne par 4 sont représentés. Ainsi, il y a parmi a, b, c, d deux entiers pairs et deux entiers impairs. La différence entre deux entiers de même parité étant paire, nous avons montré que dans ce cas aussi tous les produits considérés sont divisibles par $2 \times 2 = 4$.

Exercice 28

Les hommes sont comme les chiffres, ils n'acquièrent de la valeur que par leur position.

(Le petit théorème de Fermat)

Soit p un entier naturel premier et a un entier. Si p ne divise pas a , alors p divise $a^{p-1} - 1$.

1. Démonstration : Pour chaque entier k compris entre 1 et $p - 1$, notons r_k le reste de la division euclidienne de $k \times a$ par l'entier p . Ainsi, $ka \equiv r_k [p]$ et $0 \leq r_k \leq p - 1$.

a. Justifier que $r_k \neq 0$.

b. Montrer que, pour deux entiers k et k' quelconques, compris entre 1 et $p - 1$, si $r_k = r_{k'}$, alors $k = k'$. En déduire que l'ensemble des restes $\{r_1; r_2; \dots; r_k\}$ est confondu avec l'ensemble $\{1; 2; \dots; p - 1\}$.

c. On note $(p - 1)!$ le produit des entiers de 1 à $p - 1$.

Déduire de la question précédente que : $(p - 1)! a^{p-1} \equiv (p - 1)! [p]$

d. Justifier que p ne divise pas $(p - 1)!$ et conclure.

2. Conséquence : Démontrer que pour tout entier naturel a et tout entier premier p , $a^p \equiv a [p]$.

3. Application : Soit p un entiers supérieur ou égal à 3. Montrer que p divise $\sum_{k=0}^{p-2} 2^k$.

Corrigé

1.a. On raisonne par l'absurde: si $r_k = 0$, p divise $k \times a$; or, p est premier et ne divise pas a , donc p est premier avec a ; alors, selon le théorème de Gauss, p divise k . Mais ceci est impossible, car k est compris entre 1 et $p - 1$.

b. Si $ka \equiv r_k [p]$ et $k'a \equiv r_{k'} [p]$, alors $(k - k')a \equiv 0 [p]$; si $k' \neq k$ le même raisonnement que dans la question 1 conduit à une impossibilité. Comme $1 \leq k \leq p - 1$ et, d'après a., on a $1 \leq r_k \leq p - 1$, d'après ce qui précède, r_k prend toutes les valeurs possibles de 1 à $p - 1$.

c. En multipliant les $p - 1$ relations $ka \equiv r_k [p]$ pour $1 \leq k \leq p - 1$, on obtient alors :

$$(p - 1)! a^{p-1} \equiv (p - 1)! [p].$$

d. D'après c., p divise $(p - 1)! (a^{p-1} - 1)$. Or, p ne figure dans aucune des décompositions des facteurs du produit $(p - 1)!$, donc p ne divise pas $(p - 1)!$, donc p est premier avec $(p - 1)!$; donc, selon le théorème de Gauss, p divise $a^{p-1} - 1$.

2. Si p ne divise pas a , d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 [p]$, donc $a^p \equiv a [p]$.

Si p divise a , p divise $a^p - a$, donc $a^p \equiv a [p]$.

3. On a : $\sum_{k=0}^{p-2} 2^k = 2^{p-1} - 1$; comme p ne divise pas 2, le petit théorème de Fermat permet de conclure que p divise $2^{p-1} - 1$.

Exercice 29

Suivez les abeilles et vous mangerez le miel.

Soient m et n deux entiers et N le nombre défini par $N = mn(m^{60} - n^{60})$.

1. Donner la décomposition en facteurs premiers du nombre 56786730.

2. Montrer que N est pair.

3. En remarquant que $N = n(m^{61} - m) - m(n^{61} - n)$, montrer que 61 divise N .

4. Soit x et y deux entiers et s et t deux entiers naturels non nuls. On admet que :

$$\text{Si } s \text{ divise } t \text{ alors } x^s - y^s \text{ divise } x^t - y^t.$$

a. Montrer que pour tout $k \in \{2, 4, 6, 10, 12, 30\}$, $mn(m^k - n^k)$ divise N .

b. Montrer que pour tout $k \in \{2, 4, 6, 10, 12, 30\}$, $k + 1$ divise $mn(m^k - n^k)$.

c. En déduire que 56786730 divise $N = mn(m^{60} - n^{60})$.

Corrigé

1. On trouve sans difficulté : $56786730 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 31 \times 61$.

2. Si l'un des entiers m et n est pair, le problème est réglé. Sinon les deux entiers m et n sont impairs. Or on sait qu'un entier et ses puissances sont de même parité, ainsi m^{60} et n^{60} sont impairs et par suite $m^{60} - n^{60}$ est pair c'est-à-dire que N est donc pair.

3. On remarque que l'on peut écrire : $N = n(m^{61} - m) - m(n^{61} - n)$.

61 étant premier, on a en vertu du petit théorème de Fermat :

$$m^{61} \equiv m \pmod{61} \quad \text{et} \quad n^{61} \equiv n \pmod{61}.$$

Ainsi 61 divise $m^{61} - m$ et $n^{61} - n$ et donc 61 divise N .

4.a. On remarque que 60 est divisible par 2, 4, 6, 10, 12 et 30. Soit k l'un de ces entiers. $m^{60} - n^{60}$ est donc divisible par $m^k - n^k$ (d'après le résultat admis). D'où N est divisible par $mn(m^k - n^k)$.

b. Or $\forall k \in \{2, 4, 6, 10, 12, 30\}$, on a $p = k + 1 \in \{3, 5, 7, 11, 13, 31\}$ est premier. Il s'ensuit, selon le petit théorème de Fermat, que $p = k + 1$ divise $n^{k+1} - n$ et $m^{k+1} - m$ et donc $k + 1$ divise la combinaison linéaire $m(n^{k+1} - n) - n(m^{k+1} - m) = mn(m^k - n^k)$.

c. On vient de démontrer dans les deux items a et b de la question 4, que :

Pour tout $k \in \{2, 4, 6, 10, 12, 30\}$, $k + 1$ divise $mn(m^k - n^k)$ et $mn(m^k - n^k)$ divise N .

Donc par transitivité, pour tout $k \in \{2, 4, 6, 10, 12, 30\}$, $k + 1$ divise N autrement dit N est divisible par 3, 5, 7, 11, 13 et 31.

En conclusion, N est divisible par 2, 3, 5, 7, 11, 13, 31 et 61 et puisque ses entiers sont premiers et distincts, selon Gauss, N est divisible par leur produit 56786730.

Exercice 30

Le sommeil des sens répare le réveil de la raison.

Déterminer les deux derniers chiffres de $7^{9^{9^9}}$.

Corrigé

Soit $A = 7^{9^{9^9}}$. Connaître les deux derniers chiffres de A revient à étudier la congruence de A modulo 100. Commençons alors par étudier les puissances de 7 modulo 100.

• $7^0 = 1 [100]$, • $7^1 = 7 [100]$, • $7^2 = 49 [100]$, • $7^3 = 343 \equiv 43 [100]$, • $7^4 = 2401 \equiv 1 [100]$.

On conjecture alors que :

• $\text{Sin} \equiv 0 [4]$ alors $7^n \equiv 1 [100]$; • $\text{Sin} \equiv 1 [4]$ alors $7^n \equiv 7 [100]$;
• $\text{Sin} \equiv 2 [4]$ alors $7^n \equiv 49 [100]$; • $\text{Sin} \equiv 3 [4]$ alors $7^n \equiv 43 [100]$.

Montrons cette conjecture :

• $\text{Sin} \equiv 0 [4]$ alors il existe un entier naturel k ($n \in \mathbb{N}$) tel que $n = 4k$.

On a alors : $7^n = 7^{4k} = (7^4)^k \equiv 1^k [\text{mod } 100] \equiv 1 [\text{mod } 100]$

• $\text{Sin} \equiv 1 [4]$ alors il existe un entier naturel k ($n \in \mathbb{N}$) tel que $n = 4k + 1$.

On a alors : $7^n = 7^{4k+1} = 7 \times 7^{4k} \equiv 7 \times 1 [\text{mod } 100] \equiv 7 [\text{mod } 100]$

• $\text{Sin} \equiv 2 [4]$ alors il existe un entier naturel k ($n \in \mathbb{N}$) tel que $n = 4k + 2$.

On a alors : $7^n = 7^{4k+2} = 7^2 \times 7^{4k} \equiv 49 \times 1 [\text{mod } 100] \equiv 49 [\text{mod } 100]$

• $\text{Sin} \equiv 3 [4]$ alors il existe un entier naturel k ($n \in \mathbb{N}$) tel que $n = 4k + 3$.

On a alors : $7^n = 7^{4k+3} = 7^3 \times 7^{4k} \equiv 43 \times 1 [\text{mod } 100] \equiv 43 [\text{mod } 100]$

Il reste alors à étudier 9^{9^9} modulo 4.

On a : $9 \equiv 1 [4]$ donc pour tout entier naturel n , $9^n \equiv 1 [4]$. Par conséquent, $9^{9^9} \equiv 1 [\text{mod } 4]$. D'après l'étude précédente, on conclut alors que : $7^{9^{9^9}} \equiv 7 [100]$. Donc les deux derniers chiffres de $7^{9^{9^9}}$ sont 07.

Exercice 31

La tête ne sert pas qu'à retenir les cheveux.

Soit n un entier naturel.

1. Déterminer suivant les valeurs de n le reste de la division euclidienne de 7^n par 10.

2. Dans le système décimal, déterminer suivant les valeurs de n le chiffre des unités du nombre :

$$A = 1 + 7 + 7^2 + 7^3 + \dots + 7^n$$

Corrigé

Connaître le dernier chiffre de A revient à étudier la congruence de A modulo 10. Commençons alors par étudier les puissances de 7 modulo 10.

1. $7^2 = 49$ donc $7^2 \equiv -1 [10]$ donc $(7^2)^2 \equiv 1 [10]$ soit $7^4 \equiv 1 [10]$.

On sait que dans la division de n par 4, il existe deux entiers naturels k et r tels que $n = 4k + r$ avec $0 \leq r \leq 3$, alors : $7^n = (7^4)^k \times 7^r$ donc $7^n \equiv 7^r [10]$. D'où :

$\text{Sin} = 4k$ alors $7^n \equiv 1 [10]$;

$\text{Sin} = 4k + 1$ alors $7^n \equiv 7 [10]$;

$\text{Sin} = 4k + 2$ alors $7^n \equiv 7^2 [10]$ et donc $7^n \equiv 9 [10]$;

$\text{Sin} = 4k + 3$ alors $7^n \equiv 7^3 [10]$, or $7^3 = 7^2 \times 7$ donc $7^3 \equiv 9 \times 7 [10]$ donc $7^3 \equiv 3 [10]$, soit $7^n \equiv 3 [10]$.

2. On peut écrire : $A = 1 + 7 + 7^2 + 7^3 + 7^4(1 + 7 + 7^2 + 7^3) + \dots + 7^n$.

On a : $1 + 7 + 7^2 + 7^3 \equiv 1 + 7 - 1 - 7 \pmod{10}$ donc : $1 + 7 + 7^2 + 7^3 \equiv 0 \pmod{10}$.

Donc en conclusion :

Si $n = 4k + 3$ alors : $A = (1 + 7 + 7^2 + 7^3)(1 + 7 + \dots + 7^{4k})$ donc $A \equiv 0 \pmod{10}$;

Si $n = 4k$ alors : $A = (1 + 7 + 7^2 + 7^3)(1 + 7 + \dots + 7^{4k-4}) + 7^{4k}$ donc $A \equiv 1 \pmod{10}$;

Si $n = 4k + 1$ alors : $A = (1 + 7 + 7^2 + 7^3)(1 + 7 + \dots + 7^{4k-4}) + 7^{4k} + 7^{4k+1}$ donc :

$$A \equiv 8 \pmod{10} ;$$

Si $n = 4k + 2$ alors : $A = (1 + 7 + 7^2 + 7^3)(1 + 7 + \dots + 7^{4k-4}) + 7^{4k} + 7^{4k+1} + 7^{4k+2}$ et donc :

$$A \equiv 8 + 9 \pmod{10} \text{ et par suite } A \equiv 7 \pmod{10}.$$

Exercice 32

Peu importe la direction du vent, le soleil va toujours là où il doit aller.

1. Démontrer que pour tout entier naturel n , 42 divise $N = n(n^6 - 1)$.

2. Déterminer les entiers n tels que 84 divise $N = n(n^6 - 1)$.

Corrigé

1. On a : $42 = 3 \times 2 \times 7$ et $n(n^6 - 1) = n(n^2 - 1)(n^4 + n^2 + 1)$.

Si n est un multiple de 7 alors $n(n^6 - 1) \equiv 0 \pmod{7}$

Si n n'est pas multiple de 7, d'après le petit théorème de Fermat, on a : $n^6 - 1 \equiv 0 \pmod{7}$ et donc 7 divise $n(n^6 - 1)$.

Donc, pour tout n , 7 divise $n(n^6 - 1)$.

Si n est multiple de 3 alors $n(n^6 - 1) \equiv 0 \pmod{3}$.

Si n n'est pas multiple de 3, d'après le petit théorème de Fermat, on a : $n^2 - 1 \equiv 0 \pmod{3}$, donc $n(n^6 - 1) \equiv 0 \pmod{3}$. Pour tout n , 3 divise $n(n^6 - 1)$.

Si n est pair, on a $n(n^6 - 1)$ est multiple de 2.

Si n est impair, $n^6 \equiv 1 \pmod{2}$ donc $n(n^6 - 1) \equiv 0 \pmod{2}$.

Pour tout n , 2 divise $n(n^6 - 1)$.

Comme 2, 3 et 7 sont premiers entre eux, alors 42 divise $n(n^6 - 1)$.

2. On a : $84 = 4 \times 3 \times 7$ et d'après la question précédente, on sait que $n(n^6 - 1)$ est divisible par 3 et par 7. Donc, il suffit d'étudier la divisibilité de $n(n^6 - 1)$ par 4 car 3, 4 et 7 sont premiers entre eux deux à deux.

On divise n par 4. Les restes possibles sont 0, 1, 2 et 3.

→ Si $n \equiv 0 \pmod{4}$, alors 4 divise $n(n^6 - 1)$ donc $4 \times 3 \times 7$ divise $n(n^6 - 1)$.

→ Si $n \equiv 1 \pmod{4}$, alors $n^6 - 1 \equiv 0 \pmod{4}$ donc $4 \times 3 \times 7$ divise $n(n^6 - 1)$.

→ Si $n \equiv 2 \pmod{4}$, alors $n^6 \equiv 64 \pmod{4}$ et $n(n^6 - 1) \equiv 2 \times 63 \pmod{4}$ et $2 \times 63 = 126$ qui n'est pas multiple de 4. Donc $n(n^6 - 1)$ n'est pas multiple de 4, donc il n'est pas multiple de 84.

→ Si $n \equiv 3 \pmod{4}$, alors $n^6 \equiv 729 \pmod{4}$, $n(n^6 - 1) \equiv 3 \times 728 = 2184 \pmod{4}$ et comme $2184 = 4 \times 546$ donc 4 divise $n(n^6 - 1)$.

Conclusion : $n(n^6 - 1)$ est divisible par 84 pour tout entier n s'écrivant sous l'une des trois formes $4k$ ou $4k + 1$ ou $4k + 3$ pour k entier naturel.

Exercice 33

Quand un voleur vous embrasse, comptez vos dents.

L'objectif de l'exercice est de montrer que tout nombre impair non divisible par 5 admet un multiple qui ne s'écrit (en base 10) qu'avec des 1 (par exemple, $37 \times 1 = 37$, $37 \times 2 = 74$, $37 \times 3 = 111$). Soit n un entier naturel non nul quelconque.

Pour $k \in \mathbb{N}$, posons : $a_k = 111 \dots 1$ ($k + 1$ chiffres 1 en base 10). Notons q_k et r_k les quotient et reste de la division euclidienne de a_k par n .

1.a. Quels sont les valeurs possibles de r_k ?

b. En déduire que les entiers $r_0, r_1, \dots, r_n$ ne peuvent pas être deux à deux distincts et puis qu'il existe deux entiers s et t tels que :

$$\begin{cases} 0 \leq s < t \leq n \\ r_s = r_t \end{cases}$$

2. Montrer que n divise $a_t - a_s$.

3.a. Montrer que $a_t - a_s = a_{t-s} \times 10^{s+1}$.

b. Supposons n impair et non divisible par 5. Justifier que $\text{PGCD}(n, 10^{k+1}) = 1$.

4. Conclure.

Corrigé

1.a. On sait qu'en effectuant la division euclidienne de a_k par n , on peut écrire :

$$a_k = n \cdot q_k + r_k \quad \text{avec } 0 \leq r_k \leq n-1$$

Donc les restes possibles sont $0, 1, 2, \dots, n-1$.

b. Les $n+1$ restes $r_0, r_1, \dots, r_n$ appartiennent à l'ensemble $\{0, 1, 2, \dots, n-1\}$ de cardinal n . Donc, au moins deux restes sont confondus et par suite :

$$\exists s, t \text{ entiers tels que } \begin{cases} 0 \leq s < t \leq n \\ r_s = r_t \end{cases}$$

2. En divisant a_s et a_t par n , on peut écrire : $a_s = n \cdot q_s + r_s$ et $a_t = n \cdot q_t + r_t$. Comme $r_s = r_t$, on déduit par différence : $a_t - a_s = n \cdot (q_t - q_s)$ et donc n divise $a_t - a_s$.

3.a. On a : $a_t - a_s = \underbrace{111 \dots 111}_{t+1 \text{ chiffres } 1} - \underbrace{111 \dots 111}_{s+1 \text{ chiffres } 1} = \underbrace{111 \dots 111}_{t-s \text{ chiffres } 1} \times 10^{s+1} = a_{t-s} \times 10^{s+1}$

b. L'entier n étant impair, il est premier avec 2 et donc avec 2^{s+1} . On a également n et 5^{s+1} sont premiers entre eux. On peut donc déduire que les nombres n et $2^{s+1} \times 5^{s+1} = 10^{s+1}$ sont premiers entre eux c'est-à-dire $\text{PGCD}(n, 10^{s+1}) = 1$.

4. On sait déjà d'après la question 2 que n divise $a_t - a_s$ c'est-à-dire que n divise $a_{t-s} \times 10^{s+1}$. Comme n et 10^{s+1} sont premiers entre eux, alors Gauss nous autorise de conclure que n divise a_{t-s} .

Donc n admet un repunit comme multiple.

Exercice 34

Dieu a fait l'ébauche de l'homme au ciel; mais c'est sur la terre que chacun se crée.

Montrer que pour tout entier x , on a $x^5 \equiv x \pmod{30}$.

Corrigé

$$x^5 \equiv x \pmod{30} \Leftrightarrow x(x^4 - 1) \equiv 0 \pmod{30} \Leftrightarrow x(x^2 + 1)(x - 1)(x + 1) \equiv 0 \pmod{30}$$

On sait que $30 = 6 \times 5$ et que 5 et 6 sont premiers entre eux. D'où $x^5 - x$ est divisible par 30 si, et seulement si $x^5 - x$ est divisible à la fois par 5 et 6.

Les entiers $x, x-1$ et $x+1$ sont 3 entiers consécutifs donc leur produit est multiple de 2 et de 3 et donc de 6. D'autre part, on étudie la divisibilité par 5 en considérant les restes de la division euclidienne par 5.

→ Si x est multiple de 5 alors $x \equiv 0 \pmod{5}$;

→ Si $x \equiv 1 \pmod{5}$ alors $x - 1 \equiv 0 \pmod{5}$;

→ Si $x \equiv 2 \pmod{5}$ alors $x^2 + 1 \equiv 0 \pmod{5}$;

→ Si $x \equiv 3 \pmod{5}$ alors $x^2 + 1 \equiv 0 \pmod{5}$;

→ Si $x \equiv 4 \pmod{5}$ alors $x + 1 \equiv 0 \pmod{5}$.

Conclusion : Pour tout entier naturel x , on a donc $x^5 \equiv x \pmod{30}$.

Exercice 35

Le bruit de la mer n'empêche pas les poissons de dormir.

Soient a et b deux entiers naturels non nuls tels que $a < b$, dont le PGCD et le PPCM sont notés d et m .

On cherche à déterminer tous les couples $(a; b)$ tels que : $2m + 3d = 78$.

1. Démontrer : $2m + 3d = 78 \Leftrightarrow d(2a'b' + 3) = 78$ où a' et b' sont deux entiers premiers entre eux.

2. Trouver les valeurs possibles du couple $(d; 2a'b' + 3)$.

3. En déduire les couples $(a'; b')$.

4. Donner les couples solutions du problème.

Corrigé

1. d étant le PGCD de a et de b , il existe a' et b' entiers naturels premiers entre eux tels que :

$a = da'$ et $b = db'$. Or, d'après le cours, on a : $md = ab$ donc $md = d^2a'b'$ et $m = da'b'$.

Finalement : $2m + 3d = 78 \Leftrightarrow d(2a'b' + 3) = 78$

2. Les couples possibles $(d; 2a'b' + 3)$ sont :

$(1; 78), (2; 39), (3; 26), (6; 13), (13; 6), (26; 3), (39; 2), (78; 1)$.

On remarque que $2a'b' + 3 > 3$, ce qui permet d'éliminer les trois derniers couples.

$2a'b'$ est pair donc $2a'b' + 3$ est impair, ce qui permet d'éliminer les couples :

$(1, 78)$, $(3, 26)$ et $(13, 6)$.

Ainsi, les deux couples possibles sont : $(d = 2; 2a'b' + 3 = 39)$ et $(d = 6; 2a'b' + 3 = 13)$.

$3a'b' = 18$ ou $a'b' = 5$. Or, a' et b' sont premiers entre eux et $a' < b'$.

Pour $d = 2$, on obtient pour $(a'; b')$: $(1; 18)$ ou $(2; 9)$.

Pour $d = 6$, on obtient $(a'; b') = (1; 5)$.

4. Les couples $(a; b)$ solutions sont donc $(2; 36)$, $(4; 18)$ et $(6; 30)$.

Exercice 36

Éduquer une fille, c'est éduquer toute une nation.

Identité de Sophie Germain

1. a. n et m désignant des entiers naturels, montrer l'identité dite de Sophie Germain :

$$n^4 + 4m^4 = (n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn).$$

b. Pour quelles valeurs de n l'entier $n^4 + 4$ est-il premier ?

2. Montrer que $4^{545} + 545^4$ n'est pas un nombre premier.

Corrigé

1. a. En développant : $(n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn) = (n^2 + 2m^2)^2 - (2mn)^2 = n^4 + 4m^4$.

b. D'après l'identité précédente, on peut écrire : $n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.

L'entier $n^4 + 4$ peut toujours s'écrire comme produit de deux facteurs, donc n'est jamais premier, à moins que ... l'un de ces facteurs soit égal à 1.

→ $n^2 + 2n + 2 = 1$ équivaut à $n^2 + 2n + 1 = 0$, ce qui est le cas pour $n = -1$: l'entier vaut alors 5, qui est bien premier.

→ $n^2 - 2n + 2 = 1$ équivaut à $n^2 - 2n + 1 = 0$, ce qui est le cas pour $n = 1$: l'entier vaut alors 5, qui est bien premier.

$n^4 + 4$ n'est premier que lorsque $n = 1$ ou -1 .

2. On sait que : $4^{545} + 545^4 = 545^4 + 4 \times (4^{136})^4 = n^4 + 4m^4$ en posant $n = 545$ et $m = 4^{136}$, et d'après l'identité de Sophie Germain, on a : $4^{545} + 545^4 = (n^2 + 2m^2 + 2mn)(n^2 + 2m^2 - 2mn)$ avec $n = 545$ et $m = 4^{136}$. Il est évident que : $n^2 + 2m^2 + 2mn \neq 1$ et $n^2 + 2m^2 - 2mn \neq 1$

Donc le nombre $4^{545} + 545^4$ n'est donc pas un nombre premier.

Exercice 37

L'optimisme vient de Dieu, le pessimisme est né dans le cerveau de l'homme.

1. Soient a et b deux entiers naturels tels que $\text{PGCD}(a + b, ab) = p^2$, où p est un nombre premier.

a. Montrer que p^2 divise a^2 . En déduire que p divise a .

Montrer également que p divise b .

b. Démontrer que le PGCD de a et b est soit p soit p^2 .

2. On cherche à déterminer les entiers a et b tels que : $\begin{cases} \text{PGCD}(a + b, ab) = 49 \\ \text{PPCM}(a, b) = 231 \end{cases}$

a. Montrer que $\text{PGCD}(a, b) = 7$.

b. Quelles sont les solutions du problème posé.

Corrigé

1.a. On a :

$$\begin{aligned} \text{PGCD}(a + b, ab) = p^2 &\Rightarrow p^2 \text{ divise } (a + b) \text{ et } ab \\ &\Rightarrow p^2 \text{ divise } a(a + b) - ab = a^2 \end{aligned}$$

Mais comme p divise p^2 , donc p divise a^2 , ce qui prouve que p divise a car p est premier.

De la même manière, on démontre que p divise b .

b. Posons $\text{PGCD}(a, b) = d$.

On a : d divise a et $b \Rightarrow d$ divise $a + b$ et ab soit d divise $\text{PGCD}(a + b, ab) = p^2$.

Or comme p est premier, les seuls diviseurs naturels de p^2 sont 1, p et p^2 .

Donc $d \in \{1, p, p^2\}$. Si $\text{PGCD}(a, b) = d = 1$ alors $\text{PGCD}(a + b, ab) = 1$, ce qui est impossible.

D'où finalement : $\text{PGCD}(a, b) = p$ ou $\text{PGCD}(a, b) = p^2$.

2.a. Comme $\text{PGCD}(a + b, ab) = 49 = 7^2$, alors on est dans le cas précédent avec $p = 7$; par suite, $\text{PGCD}(a, b) = 7$ ou $\text{PGCD}(a, b) = 49$ d'après ce qui précède.

Mais, comme $\text{PGCD}(a, b)$ divise $\text{PPCM}(a, b) = 231$ et 49 ne divise pas 231, alors $\text{PGCD}(a, b) = 7$.

b. Le problème revient à chercher a et b tels que :
$$\begin{cases} \text{PGCD}(a + b, ab) = 7 \\ \text{PPCM}(a, b) = 231 \end{cases}$$

Posons $a = 7a'$ et $b = 7b'$. On sait que a' et b' sont premiers entre eux et que :

$$\text{PPCM}(a, b) = \text{PPCM}(7a', 7b') = 7 \times \text{PPCM}(a', b') = 231$$

Donc $a'b' = 33$, ce qui donne les couples $(a', b') : (1, 33), (3, 11), (11, 3)$ et $(33, 1)$, puis en multipliant par 7, on déduit les couples solutions $(a, b) : (7, 231), (21, 77), (77, 21)$ et $(231, 7)$.

Exercice 38

Cela fait du bien de rêver mais à condition de ne pas oublier de se réveiller.

Résoudre dans $\mathbb{N}$ l'équation $x^2 + x + 1 \equiv 0 [13]$.

Corrigé

1^{ère} méthode

$$x^2 + x + 1 \equiv 0 [13] \Leftrightarrow x^2 + x + 1 - 13 \equiv 0 [13] \Leftrightarrow x^2 + x - 12 \equiv 0 [13]$$

Or $x^2 + x - 12 = (x - 3)(x + 4)$, d'où :

$$x^2 + x + 1 \equiv 0 [13] \Leftrightarrow (x - 3)(x + 4) \equiv 0 [13] \Leftrightarrow 13 \text{ divise } (x - 3)(x + 4).$$

Or $\begin{cases} 13 \text{ divise } (x - 3)(x + 4) \\ 13 \text{ premier} \end{cases} \Rightarrow 13 \text{ divise } x - 3 \text{ ou } 13 \text{ divise } x + 4.$

D'où : $x = 13k + 3$ ou $x = 13k' - 4$ avec $k \in \mathbb{N}, k' \in \mathbb{N}^*$.

2^{ème} méthode

Comme on est en présence d'une équation du second degré, on peut utiliser la méthode du discriminant du moment que la base du modulo, ici 13, est un nombre premier.

On a : $\Delta = b^2 - 4ac = 1 - 4 \times 1 \times 1 = -3$. Cherchons un carré parfait congru à -3 modulo 13.

On remarque que : $\Delta = -3 \equiv 36 = 6^2 [13]$. D'où les deux solutions :

$$x_1 \equiv \frac{-1-6}{2} = \frac{-7}{2} = \frac{1}{2} \times (-7) \equiv \frac{1}{2} \times 6 = 3 [13] \text{ car } (-7) \equiv 6 [13]$$

$$x_2 \equiv \frac{-1+6}{2} = \frac{5}{2} = \frac{1}{2} \times 5 \equiv \frac{1}{2} \times (-8) = -4 [13] \text{ car } 5 \equiv -8 [13]$$

D'où les solutions : $x = 13k + 3$ ou $x = 13k' - 4$ avec $k \in \mathbb{N}, k' \in \mathbb{N}^*$.

Exercice 39

Le sourire est le parfum qui attire le plus de gens.

1. Soit a et b deux entiers relatifs et n un entier naturel supérieur ou égal à 2.

a. Montrer que l'équation $ax \equiv b [n]$ admet des solutions dans $\mathbb{Z}$ si et seulement si $\text{PGCD}(a, n)$ divise b .

b. En déduire que si n est premier et si a est un entier naturel tel que $1 \leq a < n$ alors l'équation $ax \equiv b [n]$ admet toujours des solutions entières.

c. Quelles sont parmi les équations suivantes celles qui n'admettent pas de solutions :

$$6x \equiv 8 [9] ; \quad 12x \equiv 4 [8] ; \quad 4x \equiv 9 [10] ; \quad 9x \equiv 6 [12].$$

2. Résoudre dans $\mathbb{Z}$ les équations suivantes : a. $3x \equiv 6 [7]$; b. $x^2 + 2x - 1 \equiv 2 [4]$; c. $2x^2 - 3x + 4 \equiv 3 [6]$.

Corrigé

1. a. Posons $d = \text{PGCD}(a ; n)$. Il s'agit ici d'établir une équivalence.

$\Rightarrow$ Supposons que l'équation $ax \equiv b [n]$ admet une solution entière x_0 .

x_0 solution de $ax \equiv b [n] \Rightarrow \exists k \in \mathbb{Z}$ tel que $ax_0 = b + kn$ i.e $ax_0 - kn = b$.

Comme $\begin{cases} d|a \\ d|n \end{cases}$ alors $d|ax_0 - kn$ et donc $d|b$.

$\Leftarrow$ Supposons que $d|b$.

$d|b \Rightarrow \exists k \in \mathbb{Z}$ tel que $b = kd$.

Or, selon l'identité de Bézout, d s'exprime comme combinaison linéaire de a et n i.e qu'il existe deux entiers relatifs u et v tels que $d = ua + vn$.

Donc : $b = kd = k(ua + vb) = aku + kvn$. En évaluant cette identité en modulo n , on trouve : $aku \equiv b [n]$. L'entier ku est donc solution de l'équation $ax \equiv b [n]$.

b. Si n est premier alors il est premier avec tout entiers a tel que $1 \leq a < n$, donc $\text{PGCD}(a, n) = 1$ et $\text{PGCD}(a, n)$ divise b . Donc selon la question a. l'équation $ax \equiv b [n]$ admet des solutions entières.

c. Application :

→ Pour l'équation $6x \equiv 8 [9]$, on a : $a = 6$, $b = 8$ et $n = 9$; $\text{PGCD}(6, 9) = 3$ ne divise pas 8. L'équation n'admet pas de solutions entières.

→ Pour l'équation $12x \equiv 4 [8]$, on a : $a = 12$, $b = 4$ et $n = 8$; $\text{PGCD}(12, 8) = 4$ divise 4. L'équation admet des solutions entières.

→ Pour l'équation $4x \equiv 9 [10]$, on a : $a = 4$, $b = 9$ et $n = 10$; $\text{PGCD}(4, 10) = 2$ ne divise pas 9. L'équation n'admet pas de solutions entières.

→ Pour l'équation $9x \equiv 6 [12]$, on a : $a = 9$, $b = 6$ et $n = 12$; $\text{PGCD}(9, 12) = 3$ ne divise pas 6. L'équation n'admet pas de solutions entières.

2. Résolution d'équations diophantiennes :

a. L'équation $3x \equiv 6 [7]$:

1^{ère} méthode : $3x \equiv 6 [7] \Leftrightarrow 3x - 6 \equiv 0 [7] \Leftrightarrow 7 \text{ divise } 3(x - 2)$

Comme 7 divise $3(x - 2)$ et $\text{PGCD}(7 ; 3) = 1$ alors 7 divise $x - 2$ c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x = 2 + 7k$. Donc : $S = \{2 + 7k \text{ avec } k \in \mathbb{Z}\}$.

2^{ème} méthode

On commence par chercher l'inverse de 3 modulo 7 : on remarque $3 \times 5 = 15 \equiv 1 [7]$.

Donc on multiplie la congruence par 5 (excepté le modulo) : $3x \equiv 6 [7] \xRightarrow{\times 5} x \equiv 30 [7]$, or $30 \equiv 2 [7]$

d'où : $x \equiv 2 [7]$, ...

b. L'équation $x^2 + 2x - 1 \equiv 2 [4]$:

Comme la base du modulo, ici 4, est relativement petite, on peut dresser un tableau de congruences :

$x \equiv \dots [4]$	0	1	2	3
$x^2 \equiv \dots [4]$	0	1	0	1
$2x - 1 \equiv \dots [4]$	3	1	3	1
$x^2 + 2x - 1 \equiv \dots [4]$	3	2	3	2

On remarque que $x^2 + 2x - 1 \equiv 2 [4]$ si et seulement si $x \equiv 1 [4]$ ou $x \equiv 3 [4]$.

D'où les solutions de la congruence sont les entiers de la forme $1 + 4k$ ou $3 + 4k$ avec $k \in \mathbb{Z}$.

c. L'équation $2x^2 - 3x + 4 \equiv 3 [6]$:

$$2x^2 - 3x + 4 \equiv 3 [6] \Leftrightarrow 2x^2 - 3x + 1 \equiv 0 [6]$$

On vérifie que pour tout x , on a : $2x^2 - 3x + 4 = (2x - 1)(x - 1)$. Donc un tableau de congruence permet de dégager facilement les solutions :

$x \equiv \dots [6]$	0	1	2	3	4	5
$x - 1 \equiv \dots [6]$	-1	0	1	2	3	4
$2x - 1 \equiv \dots [6]$	-1	1	3	5	7	9
$x^2 - 3x + 1 \equiv \dots [6]$	1	0	3	4	3	0

D'où les solutions sont les entiers de la forme $x \equiv 1 [6]$ ou $x \equiv 5 [6]$.

Exercice 40

Le silence a de merveilleuses choses à nous raconter.

Théorème des restes chinois

Soit p et q deux entiers naturels premiers entre eux et a et b deux entiers naturels.

1.a. Démontrer, à l'aide du théorème de Bézout, qu'il existe un entier x vérifiant le système : $\begin{cases} x \equiv a [p] \\ x \equiv b [q] \end{cases}$

b. Démontrer que si x' est un autre entiers vérifiant : $\begin{cases} x' \equiv a [p] \\ x' \equiv b [q] \end{cases}$ alors $x \equiv x' [p \times q]$.

2. **Application :** Un général décide de compter ses soldats. Il leur ordonne de se ranger en rangs de 16, il reste 3 soldats. Il leur ordonne ensuite de se ranger en rangs de 25, il reste 5 soldats.

Sachant que la troupe est constituée de moins de 400 soldats, combien y a-t-il de soldats ?

Corrigé

1.a. les entiers p et q sont premiers entre eux, donc il existe des entiers relatifs u et v tels que $up + vq = 1$ ($\otimes$), d'après le théorème de Bézout.

Posons $x = upb + vqa$ et vérifions que x satisfait le système $\begin{cases} x \equiv a [p] \\ x \equiv b [q] \end{cases}$.

On a $upa + vqa = a$ donc $vqa \equiv a [p]$. De même $upb + vqb = b$ et donc $upb \equiv b [q]$.

Finalement, on a : $x \equiv a [p]$ et $x \equiv b [q]$.

b. Soit x' une autre solution, $x \equiv x' [p]$, donc p divise $x - x'$, donc il existe $\alpha \in \mathbb{Z}$ tel que $x - x' = \alpha p$.

De même q divise $x - x'$, donc il existe $\beta \in \mathbb{Z}$ tel que $x - x' = \beta q$.

Or, d'après l'égalité (⊗), on a $(x - x')pu + (x - x')qv = x - x'$ i.e. $\beta pqu + \alpha pqv = x - x'$. Donc :

$$0 \equiv x - x' [p \times q] \text{ et par suite } x \equiv x' [p \times q].$$

2. On a $16 \times 25 = 400$, donc, d'après 1, on cherche à déterminer l'unique entier x vérifiant

$0 \leq x \leq 400$ et tel que : $\begin{cases} x \equiv 3 [16] \\ x \equiv 5 [25] \end{cases}$. A l'aide de l'algorithme d'Euclide, on trouve :

$$25 \times (-7) + 16 \times 11 = 1.$$

Ainsi, $x = 25 \times (-7) \times 3 + 16 \times 11 \times 5 \equiv 355 [400]$. Il y a donc 355 soldats.

Exercice 41

Tout le monde prie pour que la pluie tombe sur la terre mais personne ne veut se faire mouiller.

Résolution d'un système de trois congruences simultanées à une inconnue

Résoudre dans $\mathbb{Z}$ le système de congruences : (S) $\begin{cases} 5x \equiv 7 [11] & (1) \\ 7x \equiv 11 [5] & (2) \\ 11x \equiv 5 [7] & (3) \end{cases}$

Corrigé

1) Résolvons la première équation (1) de (S).

Soit $x \in \mathbb{Z}$. On cherche l'inverse de 5 modulo 11. Cet inverse existe car $5 \wedge 11 = 1$.

On remarque : $(-2) \cdot 5 = -10 \equiv 1 [11]$, donc l'inverse de 5 modulo 11 est -2 . D'où :

$$(1) 5x \equiv 7 [11] \Leftrightarrow (-2)5x \equiv (-2)7 [11] \Leftrightarrow x \equiv -3 [11] \Leftrightarrow \exists a \in \mathbb{Z}, x = -3 + 11a.$$

2) On reporte ce résultat dans la deuxième équation (2) de (S), et on raisonne comme ci-dessus (en commençant par simplifier les nombres modulo 5) :

$$\begin{aligned} (2) 7x \equiv 11 [5] &\Leftrightarrow 2x \equiv 1 [5] \Leftrightarrow 2(-3 + 11a) \equiv 1 [5] \Leftrightarrow 22a \equiv 7 [5] \Leftrightarrow 2a \equiv 2 [5] \\ &\Leftrightarrow 3(2a) \equiv 3 \times 2 [5] \Leftrightarrow a \equiv 1 [5] \Leftrightarrow \exists b \in \mathbb{Z}, a = 1 + 5b. \end{aligned}$$

$$\underbrace{3 \wedge 5 = 1}$$

On obtient : $x = -3 + 11a = -3 + 11(1 + 5b) = 8 + 55b$.

3) De même, on reporte dans l'équation (3) de (S) :

$$\begin{aligned} (3) 11x \equiv 5 [7] &\Leftrightarrow 4x \equiv 5 [7] \Leftrightarrow 4(8 + 55b) \equiv 5 [7] \Leftrightarrow 220b \equiv -27 [7] \Leftrightarrow 3b \equiv 1 [7] \\ &\Leftrightarrow 5(3b) \equiv 5 \times 1 [7] \Leftrightarrow b \equiv 5 [7] \Leftrightarrow \exists k \in \mathbb{Z}, b = 5 + 7k. \end{aligned}$$

$$\underbrace{5 \wedge 7 = 1}$$

On obtient : $x = 8 + 55b = 8 + 55(5 + 7k) = 283 + 385k$.

On conclut que l'ensemble des solutions de (S) est : $\{283 + 385k ; k \in \mathbb{Z}\}$.

Exercice 42

Face à la roche, le ruisseau l'emporte toujours, non pas par la force, mais par la persévérance.

La comète A qui est visible tous les 5 ans a été observée il y a 1 an. La comète B, visible tous les 8 ans a été observée il y a 2 ans. La comète C, visible tous les 11 ans a été observée il y a 8 ans.

Dans combien d'années pourra-t-on observer simultanément les comètes A, B et C ?

Corrigé

A sera visible dans 4 ans, 9 ans, 14 ans, ..., $4 + 5\alpha$ ans.

B sera visible dans 6 ans, 14 ans, 22 ans, ..., $6 + 8\beta$ ans.

C sera visible dans 3 ans, 14 ans, 25 ans, ..., $3 + 11\gamma$ ans.

On voit à travers ce petit schéma que dans 14 ans, on pourra observer simultanément les trois comètes.

$$\text{Cherchons } (\alpha', \beta', \gamma') \text{ tel que : } 5\alpha' + 4 = 8\beta' + 6 = 11\gamma' + 3 = x \Leftrightarrow \begin{cases} x \equiv 4 [5] \\ x \equiv 6 [8] \\ x \equiv 3 [11] \end{cases}$$

On calcule d'abord

$$\begin{cases} x_1 \equiv 1 [5] \\ x_1 \equiv 0 [8] \\ x_1 \equiv 0 [11] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 1 [5] \\ x_1 \equiv 0 [88] \end{cases} \Leftrightarrow \begin{cases} x_1 \equiv 1 [5] \\ x_1 = 88\delta \end{cases} \Leftrightarrow 88\delta \equiv 1 [5]$$

Ce qui est équivalent à :

$$3\delta \equiv 1 [5] \Leftrightarrow 6\delta \equiv 2 [5] \Leftrightarrow \delta \equiv 2 [5]$$

Donc on peut prendre $\delta = 2$ et de ce fait, on trouve $x_1 = 2 \times 88$.

On calcule ensuite :

$$\begin{cases} x_2 \equiv 0 [5] \\ x_2 \equiv 1 [8] \\ x_2 \equiv 0 [11] \end{cases} \Leftrightarrow \begin{cases} x_2 \equiv 1 [8] \\ x_2 \equiv 0 [55] \end{cases} \Leftrightarrow \begin{cases} x_2 \equiv 1 [8] \\ x_2 = 55\delta \end{cases} \Leftrightarrow 55\delta \equiv 1 [8]$$

Ce qui équivaut à : $-\delta \equiv 1 [8] \Leftrightarrow \delta \equiv -1 [8] \Leftrightarrow \delta \equiv 7 [8]$

Donc on peut prendre $\delta = 7$ et de ce fait, on trouve $x_2 = 7 \times 55$.

On calcule enfin :

$$\begin{cases} x_3 \equiv 0 [5] \\ x_3 \equiv 0 [8] \\ x_3 \equiv 1 [11] \end{cases} \Leftrightarrow \begin{cases} x_3 \equiv 1 [11] \\ x_3 \equiv 0 [40] \end{cases} \Leftrightarrow \begin{cases} x_3 \equiv 1 [11] \\ x_3 = 40\delta \end{cases} \Leftrightarrow 40\delta \equiv 1 [11]$$

Ce qui est équivalent à : $-4\delta \equiv 1 [11] \Leftrightarrow -12\delta \equiv 3 [11] \Leftrightarrow -\delta \equiv -3 [11] \Leftrightarrow \delta \equiv 8 [11]$

Donc on peut prendre $\delta = 8$ et de ce fait, on trouve $x_3 = 8 \times 40$.

Enfin, on a : $x \equiv (4 \times 2 \times 88 + 6 \times 7 \times 55 + 3 \times 8 \times 40) [5 \times 8 \times 11] \equiv 40 [440]$.

Exercice 43

L'homme qui apprend doit croire, celui qui sait doit douter.

Système non linéaire de deux congruences simultanées à une inconnue

Déterminer le plus petit entier naturel x tel que : $x \equiv 6 [23]$ et $x^2 \equiv 13 [23^2]$.

Corrigé

Soit $x \in \mathbb{Z}$. On a : $x \equiv 6 [23] \Leftrightarrow \exists y \in \mathbb{Z}$ tel que $x = 6 + 23y$. Reportons dans la deuxième congruence :

$$\begin{aligned} x^2 \equiv 13 [23^2] &\Leftrightarrow (6 + 23y)^2 \equiv 13 [23^2] \Leftrightarrow 36 + 12 \times 23y + 23^2 y^2 \equiv 13 [23^2] \\ &\Leftrightarrow 12 \times 23y \equiv -23 [23^2] \Leftrightarrow 12y \equiv -1 [23]. \end{aligned}$$

On cherche l'inverse de 12 modulo 23. Cet inverse existe car $12 \wedge 23 = 1$.

On a : $2 \times 12 = 24 \equiv 1 [23]$, donc l'inverse de 12 modulo 23 est 2. D'où :

$$12y \equiv -1 [23] \Leftrightarrow 2 \times 12y \equiv 2(-1) [23] \Leftrightarrow y \equiv -2 [23] \Leftrightarrow \exists z \in \mathbb{Z}, y = -2 + 23z.$$

Ainsi, $x \in \mathbb{Z}$ est solution du système de deux congruences si et seulement s'il existe $z \in \mathbb{Z}$ tel que :

$$x = 6 + 23(-2 + 23z) = -40 + 529z.$$

Il est alors clair que le plus petit entier naturel x convenant correspond à $z = 1$, et on a :

$$x = -40 + 529 = 489.$$

On conclut que l'entier cherché est égal à 489. On peut contrôler que 489 satisfait les congruences de l'énoncé.

Exercice 44

Quand on ne trouve pas son repos en soi-même, il est inutile de le chercher ailleurs.

Résoudre les systèmes diophantiens suivants : $(S_1) \begin{cases} x \equiv 3 [8] \\ x \equiv 7 [12] \end{cases}$ et $(S_2) \begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases}$

Corrigé

Résolution de (S_1) : Si x est solution de (S_1) $\begin{cases} x \equiv 3 [8] \\ x \equiv 7 [12] \end{cases}$ alors il existe des entiers relatifs k et k' tels que $x = 3 + 8k = 7 + 12k'$. Et donc déterminer x revient à déterminer les entiers k ou k' .

On remarque que k et k' vérifient $8k - 12k' = 7 - 3 = 4$ soit $2k - 3k' = 1$. On se retrouve avec une équation diophantienne (E) : $2k - 3k' = 1$ dont la méthode de résolution est déjà bien rodée.

1^{ère} étape : Recherche d'une solution particulière

On peut facilement voir que le couple $(-1 ; -1)$ est une solution particulière de l'équation (E).

2^{ème} étape : Recherche de toutes les solutions

Si $(k; k')$ est un couple solution de (E) alors $\begin{cases} 2k - 3k' = 1 \\ 2 \times (-1) - 3 \times (-1) = 1 \end{cases}$.

Par différence, on obtient $2(k + 1) = 3(k' + 1)$.

On en déduit alors que 3 divise $2(k + 1)$, or 2 et 3 sont premiers entre eux et donc Gauss permet de dire que 3 divise $k + 1$. D'où il existe $m \in \mathbb{Z}$ tel que $k + 1 = 3m$ soit $k = -1 + 3m$.

En remplaçant $k + 1$ par $3m$ dans l'égalité $2(k + 1) = 3(k' + 1)$, on obtient $k' = -1 + 2m$.

D'où : $x = 3 + 8k = 3 + 8(-1 + 3m) = -5 + 24m$ et donc on peut conclure que :

$$x \equiv -5 [24] \equiv 19 [24].$$

Les solutions du système (S_1) sont donc à chercher parmi les entiers x tels que $x \equiv 19 [24]$.

Réciproquement : Est-ce que tous les entiers x tels que $x \equiv 19 [24]$ sont solutions de (S_1) ?

Il est clair que $19 \equiv 3 [8]$ et $19 \equiv 7 [12]$ et donc que si $x \equiv 19 [24]$ alors $x \equiv 3 [8]$ et $x \equiv 7 [12]$ c'est-à-dire que x est solution de (S_1) $\begin{cases} x \equiv 3 [8] \\ x \equiv 7 [12] \end{cases}$.

Conclusion : L'ensemble des solutions de (S_1) $\begin{cases} x \equiv 3 [8] \\ x \equiv 7 [12] \end{cases}$ est l'ensemble des entiers de la forme :
$$x \equiv 19 [24].$$

Résolution de (S_2) :

1^{ère} méthode : Résolution du système par combinaison

On a :

$$2x - 4y \equiv 2 [6] \Leftrightarrow 2(x - 2y - 1) \equiv 0 [6] \Leftrightarrow \begin{cases} x - 2y - 1 \equiv 0 [6] \\ \text{ou} \\ x - 2y - 1 \equiv 3 [6] \end{cases}$$

En effet : si $k \in \mathbb{Z}$ et X sont tels que $2X = 6k$ alors on a les équivalences :

$$2X = 6k \Leftrightarrow X = 3k \Leftrightarrow \begin{cases} X = 3 \times 2p \text{ (si } k \text{ est pair)} \\ \text{ou} \\ X = 3 \times (2p + 1) \text{ (si } k \text{ est impair)} \end{cases}$$

D'où : $2X \equiv 0 [6] \Leftrightarrow X \equiv 0 [6] \text{ ou } X \equiv 3 [6]$.

Le système (S_2) devient alors : $\begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} \Leftrightarrow \begin{cases} x - 2y \equiv 1 [6] \\ x + 5y \equiv 2 [6] \end{cases} \text{ ou } \begin{cases} x - 2y \equiv 4 [6] \\ x + 5y \equiv 2 [6] \end{cases}$

1^{er} cas : si $\begin{cases} x - 2y \equiv 1 [6] \\ x + 5y \equiv 2 [6] \end{cases}$ alors $7y \equiv 1 [6]$ (par différence).

Il nous faut isoler y : bien entendu, il n'est pas question d'écrire que $y \equiv \frac{1}{7} [6]$.

C'est pour cette raison que l'on écrit :

$$7y \equiv 1 [6] \Leftrightarrow 7y \equiv 7 [6] \Leftrightarrow 7(y - 1) \equiv 0 [6] \Leftrightarrow 6 \text{ divise } 7(y - 1)$$

Or 6 et 7 sont premiers entre eux et le théorème de Gauss donne alors que 6 divise $y - 1$ c'est-à-dire que $y - 1 \equiv 0 [6]$ soit $y \equiv 1 [6]$.

Remarque : Attention à ne pas écrire trop hâtivement que $7y \equiv 7 [6]$ donne $y \equiv 1 [6]$ sans quoi on pensera que vous avez tout bonnement simplifié par 7 (i.e diviser les deux membres de la congruence par 7) ce qui n'est pas possible.

Finalement $y \equiv 1 [6]$ et donc $x - 2y \equiv 1 [6] \Rightarrow x \equiv 1 + 2y [6] \equiv 3 [6]$

Conclusion : Dans ce 1^{er} cas, on a : Si $\begin{cases} x - 2y \equiv 1 [6] \\ x + 5y \equiv 2 [6] \end{cases}$ alors $\begin{cases} x \equiv 3 [6] \\ y \equiv 1 [6] \end{cases}$

Remarque : Ce Si ... alors ... nous conduira automatiquement à étudier la réciproque de cette implication.

2^{ème} cas : Si $\begin{cases} x - 2y \equiv 4 [6] \\ x + 5y \equiv 2 [6] \end{cases}$ alors $7y \equiv -2 [6]$ (par différence). Il faut encore isoler y .

$$7y \equiv -2 [6] \Leftrightarrow 7y \equiv -2 + 5 \times 6 [6] \Leftrightarrow 7(y - 4) \equiv 0 [6] \Leftrightarrow 6 \text{ divise } 7(y - 4)$$

Comme 6 et 7 sont premiers entre eux alors Gauss nous autorise d'écrire que 6 divise $y - 4$ c'est-à-dire $y \equiv 4 [6]$.

Finalement $y \equiv 4 [6]$ et donc $x - 2y \equiv 4 [6] \Rightarrow x \equiv 4 + 2y \equiv 0 [6]$.

Conclusion : Dans ce 2^{ème} cas, on a : Si $\begin{cases} x - 2y \equiv 4 [6] \\ x + 5y \equiv 2 [6] \end{cases}$ alors $\begin{cases} x \equiv 0 [6] \\ y \equiv 4 [6] \end{cases}$.

Donc on peut finalement conclure que : $\begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} \Rightarrow \begin{cases} x \equiv 3 [6] \\ y \equiv 1 [6] \end{cases} \text{ ou } \begin{cases} x \equiv 0 [6] \\ y \equiv 4 [6] \end{cases}$

Réciproquement, on vérifie sans difficulté que :

$$\begin{cases} x \equiv 3 [6] \\ y \equiv 1 [6] \end{cases} \text{ et } \begin{cases} x \equiv 0 [6] \\ y \equiv 4 [6] \end{cases} \text{ sont solutions du système } \begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases}$$

Conclusion : $\begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 [6] \\ y \equiv 1 [6] \end{cases} \text{ ou } \begin{cases} x \equiv 0 [6] \\ y \equiv 4 [6] \end{cases}$

2^{ème} méthode : Résolution du système par substitution

$$\begin{aligned} \begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} &\Leftrightarrow \begin{cases} 2x - 4y \equiv 2 [6] \\ x \equiv 2 - 5y [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 - 5y [6] \\ 2(2 - 5y) - 4y \equiv 2 [6] \end{cases} \\ &\Leftrightarrow \begin{cases} x \equiv 2 - 5y [6] \\ -14y + 4 \equiv 2 [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 - 5y [6] \\ 14y \equiv 2 [6] \end{cases} \end{aligned}$$

Or $14y \equiv 2 [6] \Leftrightarrow 14y = 2 + 6k$ où $k \in \mathbb{Z} \Leftrightarrow 7y = 1 + 3k$ où $k \in \mathbb{Z}$

$$\Leftrightarrow 7y = 7 + 3(k - 2) \text{ où } k \in \mathbb{Z} \Leftrightarrow 7y \equiv 7 [3]$$

Donc $14y \equiv 2 [6] \Leftrightarrow 7y \equiv 7 [3] \Leftrightarrow 7(y - 1) \equiv 0 [3] \Leftrightarrow 3 \text{ divise } 7(y - 1)$.

Or 3 et 7 sont premiers entre eux et Gauss nous permet de dire que 3 divise $y - 1$ soit $y \equiv 1 [3]$.

Finalement, on a : $\begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 - 5y [6] \\ y \equiv 1 [3] \end{cases}$

Maintenant, on peut voir qu'il y a incompatibilité des congruences : les modulus 3 et 6 dans un même système. Pour pouvoir les combiner, il faut que les bases des congruences soient les mêmes. Pour pouvoir se dérober à cet écueil, on remarque que :

$$\begin{aligned} y \equiv 1 [3] &\Leftrightarrow y = 1 + 3k \text{ où } k \in \mathbb{Z} \Leftrightarrow \begin{cases} y = 1 + 3 \times 2p \text{ (si } k \text{ est pair)} \\ y = 1 + 3 \times (2p + 1) \text{ (si } k \text{ est impair)} \end{cases} \\ &\Leftrightarrow y \equiv 1 [6] \text{ ou } y \equiv 4 [6] \end{aligned}$$

Finalement, on a : $\begin{cases} 2x - 4y \equiv 2 [6] \\ x + 5y \equiv 2 [6] \end{cases} \Leftrightarrow \begin{cases} x \equiv 2 - 5y [6] \\ y \equiv 1 [6] \end{cases} \text{ ou } \begin{cases} x \equiv 2 - 5y [6] \\ y \equiv 4 [6] \end{cases}$

$$\Leftrightarrow \begin{cases} x \equiv 3 [6] \\ y \equiv 1 [6] \end{cases} \text{ ou } \begin{cases} x \equiv 0 [6] \\ y \equiv 4 [6] \end{cases}$$

Cette dernière équivalence étant à démontrer de la même manière que dans la première méthode.

Exercice 45

Aujourd'hui commence le reste de ta vie.

Résoudre dans $\mathbb{N}^2$ l'équation diophantienne : $3x^3 + xy + 4y^3 = 349$.

Corrigé

Soient x et y deux entiers naturels tels que $3x^3 + xy + 4y^3 = 349$.

On a $4y^3 \leq 3x^3 + xy + 4y^3 = 349$ et donc : $y \leq \sqrt[3]{\frac{349}{4}} = 4,4 \dots$

Donc $y \in \{0, 1, 2, 3, 4\}$. De même $3x^3 \leq 3x^3 + xy + 4y^3 = 349$ et donc : $x \leq \sqrt[3]{\frac{349}{3}} = 4,8 \dots$

Donc $y \in \{0, 1, 2, 3, 4\}$, ce qui ne laisse plus que $5 \times 5 = 25$ couples plausibles. Ensuite, on distingue les différents cas suivant les valeurs de y par exemple :

- $y = 0 \Rightarrow 3x^3 = 349$, équation qui ne fournit pas de solutions entières ;
- $y = 1 \Rightarrow 3x^3 + x - 345 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution ;
- $y = 2 \Rightarrow 3x^3 + 2x - 317 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution ;
- $y = 3 \Rightarrow 3x^3 + 3x - 241 = 0$, équation dont aucun des entiers de 0 à 4 n'est solution ;
- $y = 4 \Rightarrow 3x^3 + 4x - 93 = 0$, équation dont seul $x = 3$ est solution.

Donc l'ensemble des solutions est $S = \{(3, 4)\}$.

Exercice 46

La vie est comme une échelle de poulailler...courte et pleine de merde.

Soit l'équation (E) : $10x + 15y + 6z = 73$ où les inconnues x, y et z sont des entiers.

1. En utilisant des congruences convenables, montrer que si (x, y, z) est une solution de (E) alors il existe un triplet (X, Y, Z) d'entiers tel que :

$$\begin{cases} x = 3X + 1 \\ y = 2Y + 1 \\ z = 5Z + 3 \end{cases}$$

2. Montrer que (x, y, z) est solution de (E) si et seulement si (X, Y, Z) vérifie $X + Y + Z = 1$.

3. Résoudre (E) dans $\mathbb{N}$ et $\mathbb{Z}$.

Corrigé

1. Soit (x, y, z) une solution de $10x + 15y + 6z = 73$, s'il en existe. On effectue une réduction modulo 2 et on trouve $y \equiv 1 \pmod{2}$. On trouve de même $x \equiv 1 \pmod{3}$ et $z \equiv 3 \pmod{5}$.

Autrement dit, on peut nécessairement écrire : $\begin{cases} x = 3X + 1 \\ y = 2Y + 1 \\ z = 5Z + 3 \end{cases}$ avec X, Y, Z entiers

2. Réciproquement, si on écrit x, y, z sous cette forme, on a :

$$10x + 15y + 6z = 73 \Leftrightarrow 10(3X + 1) + 15(2Y + 1) + 6(5Z + 3) = 73 \Leftrightarrow X + Y + Z = 1$$

3. Résolution de (E)

• Dans $\mathbb{N}$: On remarque que si x, y, z sont dans $\mathbb{N}$, il en est de même de X, Y, Z .

Les seules solutions en (X, Y, Z) sont $(1, 0, 0)$, $(0, 1, 0)$ et $(0, 0, 1)$.

Les seules solutions en (x, y, z) sont donc $(4, 1, 3)$, $(1, 3, 3)$ et $(1, 1, 8)$.

• Dans $\mathbb{Z}$:

L'équation $X + Y + Z = 1$ a pour solutions les triplets $(X, Y, 1 - X - Y)$, avec $(X, Y) \in \mathbb{Z}^2$.

Les solutions de $10x + 15y + 6z = 73$ sont donc les (x, y, z) tels que :

$$\begin{cases} x = 3X + 1 \\ y = 2Y + 1 \\ z = 5(1 - X - Y) + 3 = 8 - 5(X + Y) \end{cases} \quad \text{avec } (X, Y) \in \mathbb{Z}^2$$

Exercice 47	Si l'ennui était mortel, l'école serait un cimetière.
--------------------	--

Résoudre dans $\mathbb{Z}^3$ le système : $\begin{cases} x - 2y + z = 0 \\ x + 2y - 2z = 1 \end{cases}$

Corrigé

Soit $(x, y, z) \in \mathbb{Z}^3$ une solution du système, s'il en existe. La deuxième équation s'écrit $x = 2(z - y) + 1$; ce qui montre que x est impair et la première équation montre alors que z est impair (somme d'un pair et d'un impair). On peut donc poser $x = 2m + 1$ et $z = 2n + 1$, avec $(m, n) \in \mathbb{Z}^2$.

Le système équivaut alors à $\begin{cases} m - y + n = -1 \\ m + y - 2n = 1 \end{cases}$ soit $\begin{cases} n = 2m \\ y = 3m + 1 \end{cases}$

L'ensemble des solutions est donc formé des triplets : $\begin{cases} x = 2m + 1 \\ y = 3m + 1 \\ z = 4m + 1 \end{cases}$ avec $m \in \mathbb{Z}$

Exercice 48	La violence est le premier refuge de l'incompétence.
--------------------	---

C'est quoi ce numéro que l'on voit sur les livres ? Ah ! c'est le numéro ISBN-13

Le numéro d'ISBN-13 (International Standard Book Number) est propre aux livres. Ils commencent en général par 978 ou 979. Les 12 premiers chiffres donnent des informations sur le pays d'origine, l'entreprise qui a produit l'ouvrage et la série de ce dernier. Le dernier chiffre est une clé de contrôle.

Le calcul de cette clé se fait de la manière suivante :

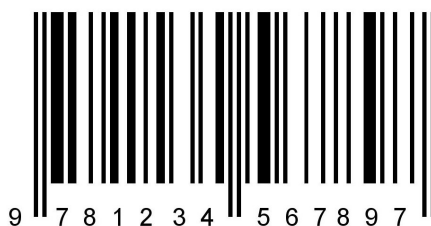
→ on somme les douze premiers chiffres du numéro, pondérés alternativement par 1 ou 3 ;

→ soit S la somme obtenue ; on calcule le reste R dans la division euclidienne de S par 10 ;

→ si $R = 0$ on pose que la clé C vaut 0 ; sinon on pose que $C = 10 - R$.

Par exemple, considérons le numéro ISBN suivant :

ISBN 978-1-234-56789-7



On pondère les douze premiers chiffres de ce numéro selon le tableau suivant:

Numéro	9	7	8	1	2	3	4	5	6	7	8	9
Pondération	1	3	1	3	1	3	1	3	1	3	1	3
Produit	9	21	8	3	2	9	4	15	6	21	8	27

La somme S des entiers de la troisième ligne du tableau vaut $S = 133$. Soit R le reste dans la division euclidienne de S par 10. On a : $S = 13 \times 10 + 3 \Rightarrow R = 3$ La clé du numéro précédent est donc $C = 10 - 3 = 7$.

Plus généralement, si on considère le code (de clé C) suivant :

$$a_1 a_2 a_3 - a_4 - a_5 a_6 a_7 - a_8 a_9 a_{10} a_{11} a_{12} - C$$

Le calcul de C se fait de la manière suivante :

→ on commence par calculer la somme S suivante : $S = \sum_{k=0}^5 a_{2k+1} + 3 \sum_{k=1}^6 a_{2k}$

→ on effectue la division euclidienne de S par 10 ; on note R le reste ;

→ si $R = 0$, on pose $C = 0$, sinon $C = 10 - R$.

1.2 Propriétés de la clé

1. Montrer que $0 \leq C \leq 9$.

2. Un livre est doté du numéro ISBN suivant :



Vérifier la valeur de la clé.

3. Montrer qu'une erreur sur un chiffre pondéré par 1 donne forcément une clé différente.

4. Montrer qu'une erreur sur un chiffre pondéré par 3 donne forcément une clé différente.

5. Montrer que si deux chiffres consécutifs diffèrent de 5, la clé reste la même en les intervertissant.

Corrigé

1. On a $0 \leq R \leq 9$. Si $R \neq 0$, alors $-9 \leq -R \leq -1 \Rightarrow 1 \leq 10 - R \leq 9$; i.e. $1 \leq C \leq 9$.

Si $R = 0$, alors $C = 0$. Dans tous les cas, $0 \leq C \leq 9$.

2. Soit S la somme définie par : $S = 9 + 7 \times 3 + 8 + 1 \times 3 + 2 + 3 \times 3 + 4 + 5 \times 3 + 6 + 7 \times 3 + 8 + 9 \times 3 = 133$

Comme $S = 13 \times 10 + 3$, avec les notations précédentes, on a $R = 3$, donc la clé cherchée est :

$$10 - R = 10 - 3 = 7.$$

3. Considérons le code (de clé C) suivant : $a_1 a_2 a_3 - a_4 - a_5 a_6 a_7 - a_8 a_9 a_{10} a_{11} a_{12} - C$ où C est la clé.

Pour calculer la clé C d'un tel numéro, on commence par calculer la somme S suivante :

$$S = \sum_{k=0}^5 a_{2k+1} + 3 \sum_{k=1}^6 a_{2k}$$

Supposons que l'on ait effectué une erreur sur un chiffre pondéré par 1, autrement dit supposons que l'un des chiffres parmi les a_{2k+1} soit faux. Soit S' la nouvelle somme obtenue ; l'entier $S' - S$ est donc un entier non nul compris au sens large entre -9 et 9 . En particulier il n'est pas divisible par 10 (car non nul !). Raisonnons par l'absurde et supposons que l'on trouve néanmoins la même valeur pour la clé. Cela revient à dire que S et S' ont le même reste dans leur division euclidienne par 10. La différence $S' - S$ est donc divisible par 10 : contradiction. La clé est donc bien différente si l'on se trompe sur l'un des a_{2k+1} .

4. Considérons le code (de clé C) suivant : $a_1a_2a_3 - a_4 - a_5a_6a_7 - a_8a_9a_{10}a_{11}a_{12} - C$ où C est la clé. Pour calculer la clé C d'un tel numéro, on commence par calculer la somme S suivante :

$$S = \sum_{k=0}^5 a_{2k+1} + 3 \sum_{k=1}^6 a_{2k}$$

Supposons que l'on ait effectué une erreur sur un chiffre pondéré par 3, autrement dit supposons que l'un des chiffres parmi les a_{2k} soit faux. Soit S' la nouvelle somme obtenue ; l'entier $S' - S$ est donc de la forme $3(a - b)$ avec a et b distincts compris entre 0 et 9. Raisonnons par l'absurde et supposons que l'on trouve néanmoins la même valeur pour la clé. Cela revient à dire que S et S' ont le même reste dans leur division euclidienne par 10 ; La différence entre les deux sommes $S' - S = 3(a - b)$ est donc divisible par 10. Donc $3|a - b|$ est divisible par 10. Comme $a \neq b$ et a, b compris entre 0 et 9, on a $1 \leq |a - b| \leq 9$; mais pour aucune de ces valeurs on obtient de multiple de 10 : contradiction. La clé est donc bien différente si l'on se trompe sur l'un des a_{2k+1} .

5. Notons S la somme initiale à calculer. Par hypothèse il existe deux nombres consécutifs a et b dans le code tels que $a - b$ est divisible par 5. La "contribution" de ces deux nombres à S est soit $3a + b$ soit $a + 3b$. Soit S' la somme obtenue en les permutant dans S . La "contribution" de ces deux nombres à S' est alors soit $a + 3b$ soit $3a + b$. On a donc : $S' - S = 2(b - a)$ ou $S' - S = 2(a - b)$. Comme 5 divise $a - b$, l'entier $S' - S$ est dans les deux cas divisible par 10. Soit r (respectivement r_0) le reste dans la division euclidienne de S par 10 (respectivement de S' par 10). Ce qui précède montre donc que $r_0 - r$ est divisible par 10. Or $|r_0 - r| < 10$, donc $r_0 - r = 0$, i.e. $r_0 = r$: la valeur de la clé reste donc inchangée si on intervertit a et b .

Exercice 49	<i>L'intelligence, c'est comme un parachute, quand on n'en a pas, on s'écrase.</i>
--------------------	---

Les entiers naturels 1, 2, 3, ..., n sont rangés dans un ordre quelconque : $a_1, a_2, a_3, \dots, a_n$.

Démontrer que si n est impair alors le produit $(a_1 - 1)(a_2 - 2) \dots (a_n - n)$ est pair.

Corrigé

La somme $(a_1 - 1) + (a_2 - 2) + \dots + (a_n - n)$ est nulle et donc paire. Comme le nombre de facteurs est impair, il est impossible qu'ils soient tous impairs donc l'un d'entre eux est pair et le produit est, par conséquent, pair.

Exercice 50	<i>Si vous pensez que l'instruction coûte cher, essayez donc l'ignorance.</i>
--------------------	--

Nombres de Carmichael ou les menteurs de Fermat

Partie A : D'après le théorème de Fermat : « Si p est entier premier, alors pour tout entier a premier avec p , $a^{p-1} \equiv 1 [p]$ ». La réciproque de ce théorème est fautive. En effet, on démontre ici l'existence de nombres entiers naturels p **non premiers** qui vérifient l'hypothèse « **pour tout entier a premier avec p , $a^{p-1} \equiv 1 [p]$** ». Ces nombres sont appelés **les nombres de Carmichael**.

Supposons qu'il existe un entier naturel n tel que : $n = p_1 \times p_2 \times \dots \times p_k$ (avec $k \geq 2$) où $p_1, p_2, \dots, p_k$ sont des nombres premiers deux à deux distincts et qui sont tels que pour $i, 1 \leq i \leq k$, $(p_i - 1)$ divise $(n - 1)$.

1. Vérifier que l'entier n n'est pas premier.

2. On considère un entier a premier avec p .

a. Démontrer que pour tout $i, 1 \leq i \leq k$, l'entier a n'est pas divisible par p_i .

b. En déduire que pour tout $i, 1 \leq i \leq k$, $a^{p_i-1} \equiv 1 [p_i]$.

c. En utilisant l'hypothèse « pour tout $i, 1 \leq i \leq k$, $(p_i - 1)$ divise $(n - 1)$ », démontrer que $\forall i \in \llbracket 1, k \rrbracket$: $a^{n-1} \equiv 1 [p_i]$.

3.a. Démontrer que $a^{n-1} \equiv 1 [n]$.

☞ On utilisera le résultat démontré à l'exercice.

b. En déduire que n est un nombre de Carmichael.

4. Montrer que 561 est un nombre de Carmichael.

Partie B : On admettra un théorème dû au mathématicien allemand Korselt :

Théorème : « Un entier naturel n supérieur à 1 non premier est un nombre de Carmichael si, et seulement si, pour tout nombre p divisant n , on a p^2 ne divise pas n et $(p - 1)$ divise $(n - 1)$ ».

1.a Écrire la décomposition en produit de facteurs premiers des nombres 561, 1 105 et 1 729. **Ces trois entiers sont les plus petits nombres de Carmichael.**

2. Soit n un nombre de Carmichael et p l'un des facteurs premiers de n .

a. Montrer que $p \equiv 1 [p-1]$, puis que $n \equiv 1 [p-1]$.

b. En écrivant n sous la forme $\left(\frac{n}{p}\right) \times p$, vérifier que $\frac{n}{p}$ est un entier et démontrer que $\frac{n}{p} \equiv 1 [p-1]$.

c. En déduire que si p est un facteur premier d'un nombre de Carmichael n , alors le produit des autres facteurs premiers est congru à 1 modulo $(p-1)$.

3. A l'aide de la question précédente, démontrer qu'un nombre de Carmichael ne peut pas être le produit de deux nombres premiers.

Conséquence : Un nombre de Carmichael est le produit d'au moins trois nombres premiers deux à deux distincts.

4. Démontrer que tout nombre de Carmichael est impair.

Corrigé

Partie A

1. L'entier n est un produit d'au moins deux nombres premiers distincts ($k \geq 2$), donc il n'est pas premier.

2.a. S'il existe un facteur p_i qui divise a , alors comme p_i divise n , a et n ne seraient pas premiers entre eux. Donc aucun des facteurs p_i ne divise a .

b. L'entier a est premier avec p_i pour tout i , $1 \leq i \leq k$, donc, d'après le petit théorème de Fermat, $a^{p_i-1} \equiv 1 [p_i]$.

c. D'après l'hypothèse, pour tout entier i , $1 \leq i \leq k$, $(p_i - 1)$ divise $(n - 1)$, il existe un entier k_i tel que l'on ait $(n - 1) = k_i(p_i - 1)$. D'où $a^{k_i(p_i-1)} \equiv 1^{k_i} [p_i]$, donc, pour tout entier i , $1 \leq i \leq k$, $a^{n-1} \equiv 1 [p_i]$.

3.a. L'entier $a^{n-1} - 1$ est divisible par tous les nombres premiers p_i , donc d'après l'exercice 13, il est divisible par leur produit. Et donc finalement, $a^{n-1} - 1 \equiv 0 [n]$ ce qui signifie que $a^{n-1} \equiv 1 [n]$.

b. L'entier n est non premier et vérifie, «pour tout entier a premier avec p , $a^{p-1} \equiv 1 [p]$ », c'est un nombre de Carmichael.

4. On a : $561 = 3 \times 11 \times 17$. On a 2 divise 560, 10 divise 560 et 16 divise 560, donc 561 est un nombre de Carmichael.

Partie B

1.a. b. $561 = 3 \times 11 \times 17$ avec 3^2 , 11^2 et 17^2 qui ne divisent pas 561, et 2 divise 560, 10 divise 560, 16 divise 560 ; $1105 = 5 \times 13 \times 17$ avec 5^2 , 13^2 et 17^2 qui ne divisent pas 1 105 et 4 divise 1104, 12 divise 1104, 16 divise 1104 ; $1729 = 7 \times 13 \times 19$ avec 7^2 , 13^2 et 19^2 qui ne divisent pas 1 729 et 6 divise 1728, 12 divise 1728, 18 divise 1728.

2.a. De façon évidente, $p-1 \equiv 0 [p-1]$ et $n-1 \equiv 0 [p-1]$, car l'entier $p-1$ divise $n-1$. Donc :

$$p \equiv 1 [p-1] \text{ et } n \equiv 1 [p-1].$$

b. Comme p intervient dans la décomposition en facteurs premiers de n , on a p divise n et $\frac{n}{p}$ est un entier. Ainsi, $n = \frac{n}{p} \times p \equiv \frac{n}{p} [p-1]$ et comme $n \equiv 1 [p-1]$, alors $\frac{n}{p} \equiv 1 [p-1]$.

c. Comme l'entier p^2 ne divise pas n , le produit des autres facteurs premiers est $\frac{n}{p}$ et il est congru à 1 [modulo $p-1$].

3. Supposons que $n = pq$ soit un nombre de Carmichael (p et q premiers). D'après la question 2.c., on aurait $q \equiv 1 [p-1]$ et $p \equiv 1 [q-1]$, donc $p-1$ serait un multiple de $q-1$ et $q-1$ un multiple de $p-1$; donc on aurait $p = q$ et $n = p^2$ ce qui contredirait le théorème de Korselt, car p^2 diviserait n .

4. Comme un nombre de Carmichael a au moins trois facteurs premiers distincts, il en a au moins un impair ; soit p ce facteur premier impair. Alors, comme $p-1$ divise $n-1$ et que $p-1$ est pair, on a $n-1$ pair, i.e n impair.

Exercice 51

Aucun homme n'a assez de mémoire pour réussir dans le mensonge.

Dans le système décimal, on donne $\overline{23}_{(dix)}$, $\overline{32}_{(dix)}$, $\overline{47}_{(dix)}$, $\overline{100}_{(dix)}$.

Écrire ces nombres dans les systèmes binaire et hexadécimal.

Corrigé

→ On peut poser les divisions :

$$\begin{array}{r} 23 \overline{) 2} \\ 1 \\ \underline{11} \\ 1 \\ \underline{5} \\ 1 \\ \underline{2} \\ 0 \\ \end{array}$$

$$\begin{array}{r} 23 \overline{) 16} \\ 7 \\ \underline{7} \\ 1 \end{array}$$

On peut aussi écrire :

$$23 = 2^4 + 2^2 + 2 + 1 \text{ donc } \overline{23}_{(dix)} = \overline{10111}_{(deux)} \text{ et } 23 = 16 \times 1 + 7 \text{ donc } \overline{23}_{(dix)} = \overline{17}_{(seize)}.$$

$$\rightarrow 32 = 2^5 \text{ et } 23 = 16 \times 2, \text{ donc } \overline{32}_{(dix)} = \overline{100000}_{(deux)} \text{ et } \overline{32}_{(dix)} = \overline{20}_{(seize)}.$$

$$\rightarrow 47 = 2^5 + 2^3 + 2^2 + 2 + 1 \text{ et } 47 = 16 \times 2 + 15 \text{ donc :}$$

$$\overline{47}_{(dix)} = \overline{101111}_{(deux)} \text{ et } \overline{47}_{(dix)} = \overline{2F}_{(seize)}.$$

$$\rightarrow 100 = 2^6 + 2^5 + 2^2 \text{ et } 100 = 16 \times 6 + 4 \text{ donc :}$$

$$\overline{100}_{(dix)} = \overline{1100100}_{(deux)} \text{ et } \overline{100}_{(dix)} = \overline{64}_{(seize)}.$$

Exercice 52**Quand le sage montre la Lune, l'abruti regarde le doigt.**

Déterminer tous les nombres dont l'écriture en base sept est de la forme $\overline{xyz}$ et l'écriture en base onze est $\overline{zyx}$.

Corrigé

Si n est un nombre qui s'écrit $\overline{xyz}$ en base sept et $\overline{zyx}$ en base onze, on a alors :

$$n = z + y \times 7 + x \times 7^2 = 49x + 7y + z$$

$$= x + y \times 11 + z \times 11^2 = 121z + 11y + x$$

Ce qui donne l'égalité : $30z + y = 12x$.

D'autre part, comme x, y et z sont des chiffres de la base sept, alors on a les conditions : $0 \leq x \leq 6$, $0 \leq y \leq 6$ et $0 \leq z \leq 6$; d'où le système :

$$\begin{cases} 30z + y = 12x \\ 0 \leq x \leq 6 \\ 0 \leq y \leq 6 \\ 0 \leq z \leq 6 \end{cases}$$

On remarque que y est multiple de 6 car $y = 6(2x - 5z)$. D'où $y = 0$ ou $y = 6$.

→ Pour $y = 0$, la relation $30z + y = 12x$ devient $30z = 12x$ soit $5z = 2x$. On trouve deux solutions de $5z = 2x$ dans $\llbracket 0; 6 \rrbracket$ à savoir : $(x = 0 \text{ et } z = 0)$ et $(x = 5 \text{ et } z = 2)$

→ Pour $y = 6$, la relation $30z + y = 12x$ devient $5z = 2x - 1$. Cette relation assure que z est impair car 5 et $2x - 1$ le sont. Par suite les seules valeurs possibles pour z sont : 1, 3 ou 5.

- Pour $z = 1$, on a $2x - 1 = 5$ soit $x = 3$;
- Pour $z = 3$, on a $2x - 1 = 15$ soit $x = 8$ à rejeter ;
- Pour $z = 5$, on a $2x - 1 = 25$ soit $x = 13$ à rejeter.

Dans ce cas, la seule solution acceptable est $(x = 3 \text{ et } z = 1)$.

Ainsi, le problème admet trois solutions :

$$\overline{000}_{(sept)} = \overline{000}_{(onze)} = \overline{000}_{(dix)}$$

$$\overline{502}_{(sept)} = \overline{205}_{(onze)} = \overline{247}_{(dix)}$$

$$\overline{361}_{(sept)} = \overline{163}_{(onze)} = \overline{190}_{(dix)}$$

Exercice 53**Je travaille à être heureux : c'est le plus beau des métiers.**

Trouver les nombres premiers dont l'écriture en base b utilise une fois et une seule tous les chiffres possibles de la base de numération (le 0 est possible en tête).

Corrigé

Si $b = 2$, la seule solution est $n = \overline{10} = 2$.

Si $b = 3$, seuls $n = \overline{012} = 5$, $n = \overline{021} = 7$, $n = \overline{102} = 11$ et $n = \overline{201} = 19$ conviennent.

Soit n un entier dont l'écriture en base $b > 4$ utilise une seule fois tous les chiffres de la base. Il est clair qu'alors n est strictement supérieur à b (il a au moins deux chiffres non nuls).

On peut écrire $n = \sum_{k=0}^{b-1} a_k b^k$, avec $\{a_0, a_1, \dots, a_{b-1}\} = \{0, 1, \dots, b-1\}$.

Dans ces conditions : $n = \sum_{k=0}^{b-1} a_k + \sum_{k=0}^{b-1} a_k (b^k - 1) = \frac{b(b-1)}{2} + \sum_{k=0}^{b-1} a_k (b^k - 1)$

- Si b est pair ($b = 2m$ avec $m > 2$) alors on voit que n est divisible par $b-1$.

- Si b est impair ($b = 2m+1$ avec $m > 2$), alors on voit que n est divisible par m .

Dans les deux cas, on constate que n n'est pas premier.

Les seules solutions sont donc celles obtenues pour $b = 2$ et $b = 3$.

Exercice 54

Le peu que je sais, c'est à mon ignorance que je le dois.

Déterminer la base x pour que le nombre $\overline{171}_x$ écrit en base dix soit un carré parfait.

Corrigé

Au prime abord, on remarque que, comme le chiffre 7 figure dans l'écriture du nombre en base x , alors on a $x \geq 8$. D'autre part, on suppose que $\overline{171}_x$ est le carré d'un entier n , alors on doit avoir, $\overline{171}_x = n^2$, soit $1 + 7x + x^2 = n^2$, ou encore : $x^2 + 7x + (1 - n^2) = 0$, avec $x \in \mathbb{N}$.

Pour que l'équation possède des solutions, il faut que son discriminant soit un carré parfait :

$\Delta = 49 - 4(1 - n^2) = k^2 \Leftrightarrow k^2 - 4n^2 = 45 \Leftrightarrow (k - 2n)(k + 2n) = 45$ avec k et n des entiers naturels non nuls.

Donc $k - 2n$ et $k + 2n$ sont des diviseurs « complémentaires » de 45, avec bien entendu la double inégalité : $k - 2n < k + 2n$. Comme $45 = 1 \times 45 = 3 \times 15 = 5 \times 9$ alors on a : $(k - 2n; k + 2n) \in \{(1; 45), (3; 15), (5; 9)\}$.

Examinons ces couples au cas par cas :

$\rightarrow \begin{cases} k - 2n = 1 \\ k + 2n = 45 \end{cases} \Rightarrow k = 23, n = 11 \text{ et } x = 8; \text{ solution acceptable.}$

$\rightarrow \begin{cases} k - 2n = 3 \\ k + 2n = 15 \end{cases} \Rightarrow k = 9, n = 3 \text{ et } x = 1; \text{ solution à rejeter.}$

$\rightarrow \begin{cases} k - 2n = 5 \\ k + 2n = 9 \end{cases} \Rightarrow k = 7, n = 1 \text{ et } x = 0; \text{ solution à rejeter}$

Il en résulte que, en base huit, la configuration 171 représente un carré parfait.

En effet, on a : $\overline{171}_{(hu)} = 1 + 7 \times 8 + 1 \times 8^2 = 121 = 11^2$.

Exercice 55

A tout problème il y a 2 solutions : La bonne et celle de l'École de Guerre.

Soit $n = \overline{abcd}_{dix}$ un carré parfait à quatre chiffres, tous inférieurs ou égaux à 6. Si on ajoute 3 à chacun des ces chiffres, on obtient encore un carré parfait m . On note r et s les racines carrées respectives de n et m .

1. Montrer que $m = n + 3333$.

2. En déduire un majorant de chacun des deux nombres r et s .

3. En exploitant la décomposition de 3333, trouver n .

Corrigé

1. On sait que $n = a \times 10^3 + b \times 10^2 + c \times 10 + d$, où a, b, c, d sont dans $\{0, 1, 2, 3, 4, 5, 6\}$ (bien sûr $a \geq 1$).

On obtient le nombre m en ajoutant 3 à tous les chiffres de n , ce qui donne la décomposition de m en base dix :

$$m = (a + 3) \times 10^3 + (b + 3) \times 10^2 + (c + 3) \times 10 + (d + 3)$$

Soit : $m = [a \times 10^3 + b \times 10^2 + c \times 10 + d] + [3 \times 10^3 + 3 \times 10^2 + 3 \times 10 + 3] = n + 3333$.

2. Les entiers n et m étant des carrés parfaits, il existe deux entiers r et s tels que : $r^2 = n$ et $s^2 = m$. On a de toute évidence $n < 6666$ et donc $m = n + 3333 < 9999$ (6666 et 9999 ne sont pas des carrés parfaits). Donc : $r^2 < 6666$ et $s^2 < 9999$ et par suite $r < \sqrt{6666}$ et $s < \sqrt{9999}$; soit enfin :

$$r \leq 81 \text{ et } s \leq 99.$$

3. L'égalité $m = n + 3333$ se traduit par $s^2 = r^2 + 3333$ ou encore : $s^2 - r^2 = 3333 = 3 \times 11 \times 101$
D'où : $(s - r)(s + r) = 3 \times 11 \times 101$ avec $0 < s - r < s + r$
La seule possibilité est donc $\begin{cases} s - r = 33 \\ s + r = 101 \end{cases}$; ce qui donne $r = 34$ et $s = 67$.
Donc la valeur de n est $n = r^2 = 34^2 = 1156$.

Exercice 56

L'avantage d'être intelligent, c'est qu'on peut toujours faire l'imbécile, alors que l'inverse est totalement impossible.

Soit n un entier se terminant par 6. Si on déplace ce chiffre 6 pour le placer en tête de l'écriture décimale de n alors on obtient l'entier m . On écrit $n = 10p + 6$ avec p dans $\mathbb{N}$.

1. Donner une expression de m en fonction de p et d où d est le nombre de chiffres de n en base dix.

2. On suppose que $m = 4n$.

a. Montrer alors que p est pair et que $10^{d-1} - 4 = 13q$ où q est l'entier tel que $p = 2q$.

b. En étudiant les restes de la division euclidienne des puissances de 10 par 13, déterminer la valeur minimale de d tel que $10^{d-1} \equiv 4 \pmod{13}$.

3. En déduire les deux plus petites valeurs de n telles que $m = 4n$.

Corrigé

1. Si $n = 10p + 6$ alors en plaçant le chiffre 6 en tête de l'écriture décimale de n , on obtient l'entier naturel $m = 6 \times 10^{d-1} + p$ où d est le nombre de chiffres de n en base dix.

2. a. On a : $m = 4n \Leftrightarrow 6 \times 10^{d-1} + p = 4(10p + 6) \Leftrightarrow 6 \times 10^{d-1} - 24 = 39p$

En simplifiant la dernière expression par 3, on trouve : $2 \times 10^{d-1} - 8 = 13p$. Le 1^{er} membre de cette égalité étant pair et 13 impair alors p est nécessairement pair et par suite on peut se permettre d'écrire $p = 2q$.

En réécrivant l'égalité $2 \times 10^{d-1} - 8 = 13p$ avec $p = 2q$ et puis en simplifiant par 2, on aboutit au résultat demandé : $10^{d-1} - 4 = 13q$.

b. On vérifie qu'en modulo 13, on a : $10^0 \equiv 1, 10^1 \equiv 10, 10^2 \equiv 9, 10^3 \equiv 12, 10^4 \equiv 3, 10^5 \equiv 4$

Ainsi l'entier d minimal tel que $10^{d-1} \equiv 4 \pmod{13}$ est égal à 6 et par conséquent : $q = \frac{10^{6-1} - 4}{13} = 7\,692$

3. D'après ce qui vient d'être établi, on peut dire que la valeur minimale de n est $n = 20q + 6$ avec $q = 7\,692$. Ce qui donne $n = 153\,846$. La deuxième valeur de n se déduit de la 2^{ème} valeur de q et donc de la deuxième valeur possible de l'entier d . Or, la 2^{ème} valeur de d est 12 car : $10^{12-1} \equiv 10^{11} \equiv 10^6 \times 10^5 \equiv 1 \times 4 \equiv 4 \pmod{13}$.

D'où enfin :

$$q = \frac{10^{11} - 4}{13} = 7\,692\,307\,692 \text{ et donc } n = 20q + 6 = 153\,846\,153\,84.$$

Exercice 57

L'avantage d'un médecin, c'est que lorsqu'il commet une erreur, il l'enterre tout de suite.

Soit $b \geq 3$ une base de numération. Montrer que le nombre $n = \overline{12 \dots 21}_b$ où le chiffre 2 est répété $p - 2$ fois, est non premier.

Corrigé

On a :

$$\begin{aligned} n &= 1 + 2b + \dots + 2b^p + b^{p+1} \\ &= 1 + 2b \frac{b^p - 1}{b - 1} + b^{p+1} \\ &= \frac{b^{p+2} + b^{p+1} - b - 1}{b - 1} \\ &= \frac{(b^{p+1} - 1)(b + 1)}{b - 1} \\ &= (1 + b + \dots + b^p)(b + 1) \end{aligned}$$

Les deux termes de ce produit étant supérieurs à 2, le nombre n n'est pas premier.

Exercice 58	Une mauvaise herbe, c'est une plante dont les vertus n'ont pas encore été découvertes.
--------------------	---

Soit un entier naturel N . On note d le nombre de chiffres de son écriture décimale et b le nombre de chiffres de son écriture binaire.

1. Encadrer N par deux puissances de 10 consécutives puis par deux puissances de 2 consécutives.
2. Démontrer que $3d - 2 \leq b \leq 4d$.
3. Indiquer un encadrement du nombre de chiffres de l'écriture binaire de l'entier $\overline{7\,218\,917}_{(dix)}$.

Corrigé

1. Par définition de d et b , on a : $10^{d-1} \leq N < 10^d$ et $2^{b-1} \leq N < 2^b$.
2. On a $2^{3d-3} = 8^{d-1}$ et $8^{d-1} < 10^{d-1} \leq N < 10^d < 16^d$ et $16^d = 2^{4d}$.
D'où : $2^{b-1} \leq N < 2^b \Rightarrow 3d - 3 \leq b - 1$ et $b \leq 4d$
 $\Rightarrow 3d - 2 \leq b \leq 4d$

Donc : $3d - 2 \leq b \leq 4d$.

3. Dans ce cas, on a $d = 7$ et par suite $3 \times 7 - 2 \leq b \leq 4 \times 7$ c'est-à-dire : $19 \leq b \leq 28$.

Exercice 59	Cessez de vouloir tout comprendre. Il n'est nul besoin de tout savoir sur l'océan pour y nager.
--------------------	--

Alice et Bob jouent à un jeu : Bob pense à un polynôme P à coefficients entiers positifs et Alice doit le deviner. À chaque tour, Alice demande la valeur de P en un nombre entier, et Bob la lui donne. En combien de tours Alice pourra-t-elle deviner P ? (Précisons qu'Alice sait que les coefficients de P sont des entiers positifs, mais qu'elle n'en sait pas plus. En particulier, elle n'a aucune information sur son degré.)

Corrigé

Alice peut déterminer le polynôme avec seulement deux questions. Pour cela, remarquons que si $P(X) = \sum_{k=0}^d a_k X^k$, avec $a_k \in \mathbb{N}$ et qu'un entier n est strictement plus grand que tous les a_k , la donnée de $P(n)$ détermine le polynôme P : $P(n) = \sum_{k=0}^d a_k n^k$ et les a_k sont simplement les « chiffres » de l'écriture de $P(n)$ en base n . Ainsi, Alice peut poser la première question « Combien vaut $P(1)$? » La réponse de Bob est $P(n) = \sum_{k=0}^d a_k$, qui est évidemment plus grand (au sens large) que les coefficients a_k . Alice n'a alors plus qu'à prendre n'importe quel entier $n > P(1)$ et à demander la valeur de $P(n)$.

Exercice 60	Peu importe où nous posons le pied, un chemin naît sous nos pas.
--------------------	---

Montrer que tout entier naturel n peut s'écrire de façon unique sous la forme :

$$n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_d d! + \cdots$$

où $a_1, a_2, a_3, \dots$ sont des entiers tels que $0 \leq a_i \leq i$ pour tout i .

☞ On raisonne comme pour la décomposition en base b . Penser à la division euclidienne.

Corrigé

On remarque que si n s'écrit sous la forme : $n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_d d! + \cdots$

avec $0 \leq a_i \leq i$, alors a_1 est forcément le reste de la division euclidienne de n par 2 puisque la somme $a_2 2! + a_3 3! + \cdots$ est un multiple de 2. On pose donc la division euclidienne de n par 2 et on écrit : $n = 2q_1 + a_1$ pour des entiers q_1 et a_1 avec $0 \leq a_1 \leq 1$. Il s'agit maintenant d'écrire q_1 sous la forme :

$$q_1 = a_2 \frac{2!}{2} + a_3 \frac{3!}{2} + \cdots + a_d \frac{d!}{2} + \cdots$$

et pour cela on considère la division euclidienne de q_1 par 3. On écrit : $q_1 = 3q_2 + a_2$ pour des entiers q_2 et a_2 avec $0 \leq a_2 \leq 2$. On veut alors écrire q_2 sous la forme :

$$q_2 = a_3 \frac{2!}{3!} + a_4 \frac{4!}{3!} + \cdots + a_d \frac{d!}{3!} + \cdots$$

et on considère donc la division euclidienne de q_2 par 4, obtenant ainsi q_3 et a_3 .

La suite des q_i est une suite d'entiers positifs et si $q_i > 0$, alors $q_{i+1} < q_i$. Il existe donc un entier d tel que $q_d = 0$ et à ce moment on a l'égalité : $n = a_1 1! + a_2 2! + a_3 3! + \cdots + a_{d-1} (d-1)!$

Pour l'unicité, on remarque en analysant la construction précédente, qu'à chaque étape, on n'avait qu'un seul choix pour α_i .

Exercice 61

Les professeurs ouvrent la porte, mais vous devez entrer par vous-même.

Le code CLE (Codage Large Échelle)

I. Le système binaire et la base 2

Le système de numération que nous utilisons habituellement est le système décimal, les nombres y sont écrits en base 10 : $7896 = 7 \times 10^3 + 8 \times 10^2 + 9 \times 10^1 + 6 \times 10^0$

Pour écrire les nombres, on utilise les 10 chiffres : 0; 1; 2; 3; 4; 5; 6; 7; 8 et 9 mais on peut aussi choisir d'autres bases, par exemple la base 2. Les seuls chiffres utilisés sont alors 0 et 1.

Par exemple : le nombre qui s'écrit 10111 en base 2, s'écrit : $1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$

Pour passer de l'écriture en base 10 à l'écriture en base 2, on effectue les divisions successives par 2:

D'où, en remontant les restes des divisions successives : $67 = 1000011$ en base 2.

Autre façon : tableau du système linéaire :

$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
1	0	0	0	0	1	1

On a : $67 = 64 + 3$ et $3 = 2 + 1$ donc $67 = 2^6 + 2^1 + 2^0$.

1. Écrire en base 10 le nombre qui s'écrit 1000101110 en base 2.
2. Écrire en base 2 le nombre qui s'écrit 157 en base 10. Même question pour 10 en base 10.
3. Faire la table d'addition et la table de multiplication de la base 2. (Utiliser les tables suivantes)

$\begin{smallmatrix} + \\ \sim \end{smallmatrix}$	0	1	2	3
0				
1				
2				
3				

et

$\times$ $\simeq$	0	1	2	3
0				
1				
2				
3				

4. Calculer en base 2 : $1101101 + 1011011$ puis 101101×10011011 . Donner alors les règles simples de l'addition et de la multiplication dans le système binaire.
5. D'après ce qui précède, quelles sont les avantages et les inconvénients du système binaire ?

II. Le Code CLE

Notre système de numération ne permet pas à la calculatrice d'obtenir la valeur exacte du produit $123125256 \times 785698254$; on en a seulement une valeur approchée.

Pour pallier cet inconvénient, on a cherché d'autres façons d'écrire les nombres. L'une d'entre elles s'appelle le code CLE (Code à Large Échelle).

Sur un exemple : Le nombre 67 en base 10 s'écrit 100011 en base 2. En effet on a la décomposition binaire suivante : $67 = 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$ c'est-à-dire : $67 = 2^6 + 2^1 + 2^0$. Ainsi 67 s'écrit alors en code CLE sous la forme (6; 1; 0).

1.a. Écrire en base 10 le nombre (7; 5; 3; 1)

b. Écrire en code CLE les nombres en base 10 suivants : 359, 250 et 128.

2. Premières propriétés : nature du nombre

a. A quoi reconnaît-on qu'un nombre écrit en code CLE est impair ?

b. A quoi reconnaît-on qu'un nombre écrit en code CLE est pair ?

c. A quoi reconnaît-on qu'un nombre écrit en code CLE est une puissance de 2 ?

3. Propriétés de l'addition

a. Peut-on facilement additionner les nombres écrits en code CLE ?

b. Écrire en code CLE la somme $(15)_{CLE} + (15)_{CLE}$, puis la somme : $(n)_{CLE} + (n)_{CLE}$.

c. Écrire en code CLE :

$(11; 5; 3; 0)_{CLE} + (34; 11; 5; 3)_{CLE}$ puis $(18; 16; 8; 4; 3; 2)_{CLE} + (19; 16; 9; 4; 3; 2; 1)_{CLE}$.

d. Peut-on énoncer une règle générale ?

4. Propriétés de la multiplication

a. Peut-on facilement multiplier les nombres écrits en code CLE ?

b. Écrire en code CLE le produit $(n)_{CLE} \times (m)_{CLE}$ où n et m sont deux entiers naturels.

c. Écrire en code CLE : $(5; 2; 0)_{CLE} \times (4)_{CLE}$ puis $(5; 3)_{CLE} \times (7; 2; 1)_{CLE}$.

d. Peut-on énoncer une règle générale ?

e. Écrire en code CLE le carré : $(12; 4)_{CLE}^2$.

Corrigé

1. 1000101110 = $2^9 + 2^5 + 2^3 + 2^2 + 2^1 = 558$.

2. $157 = 128 + 16 + 8 + 4 + 1 = 2^7 + 2^4 + 2^2 + 2^0$ s'écrit donc 10010101.

3. Vu qu'en base 2, on a : $2 = 2^1 = 10$, $3 = 2^1 + 2^0 = 11$, $4 = 2^2 = 100$, $5 = 2^2 + 2^0 = 101$, $6 = 2^4 + 2^1 = 110$, $9 = 2^3 + 2^0 = 1001$, on peut compléter le tableau suivant :

$+$ $\sim$	0	1	2	3		$\times$ $\sim$	0	1	2	3
0	0	1	10	11		0	0	0	0	0
1	1	10	11	100	et	1	0	1	10	11
2	10	11	100	101		2	0	10	100	101
3	11	100	101	110		3	0	11	101	1001

4. Calcul en base 2 de $1101101 + 1011011$ puis de 101101×10011011 :

On peut disposer les calculs comme à l'accoutumée :

$$\begin{array}{r}
 \begin{array}{r}
 1101101 + 1011011 = \\
 \begin{array}{r}
 \begin{array}{cccccccc}
 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
 + & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 \hline
 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
 \text{retenue} & 1 & 1 & 1 & 2 & 2 & 1 & 0 & 0 & 0 & 0
 \end{array} \\
 \begin{array}{cccccccc}
 & & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
 \times & & & & & 1 & 0 & 1 & 1 & 0 & 1 \\
 \hline
 & & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & & & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & & & & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
 \hline
 & & & & & & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
 \end{array}
 \end{array}
 \end{array}
 \end{array}$$

5. Les calculs en base 2 se font plus vite mais il y a beaucoup plus d'opérations à faire. Dans le système informatique, les processeurs, au cœur des ordinateurs, gèrent des 0 (éteint) et des 1 (allumé), par le biais d'une myriade de microtransistors, à coup de 3 GHz (soit 3×10^9 opérations par seconde !).

II. 1.a. $(7; 5; 3; 1)_{CLE} = 2^7 + 2^5 + 2^3 + 2^1 = 170$.

b. $359 = 101100111 = 2^9 + 2^7 + 2^6 + 2^2 + 2^1 + 2^0 = (9; 7; 6; 2; 1; 0)_{CLE}$.

$250 = 11111010 = (7; 6; 5; 4; 3; 1)_{CLE}$

$128 = 10000000 = (7)_{CLE}$.

2. Propriétés du nombre

a. Un nombre écrit en code CLE est impair s'il se termine par 0.

b. Un nombre écrit en code CLE est pair s'il ne se termine pas par 0.

c. Un nombre écrit en code CLE est une puissance de 2 s'il est de la forme $(n)_{CLE}$.

3. Propriétés de l'addition

a. Cela dépend des nombres mis en jeu.

b. $(15)_{CLE} + (15)_{CLE} = 2^{15} + 2^{15} = 2 \times 2^{15} = 2^{16} = (16)_{CLE}$.

$(n)_{CLE} + (n)_{CLE} = 2^n + 2^n = 2 \times 2^n = 2^{n+1} = (n+1)_{CLE}$.

c. $(11; 5; 3; 0)_{CLE} + (34; 11; 5; 3)_{CLE} = (34; 12; 6; 4; 3; 0)_{CLE}$.

$(18; 16; 8; 4; 3; 2)_{CLE} + (19; 16; 9; 4; 3; 2; 1)_{CLE} = (19; 18; 17; 9; 8; 5; 4; 3; 1)_{CLE}$.

d. Règle générale pour effectuer la somme de deux nombres CLE

On ajoute de droite à gauche, tout chiffre présent une fois dans l'un des 2 nombres est à marquer dans la somme. Si un chiffre est dans les 2 nombres, on écrit son suivant dans la somme. Il faudra peut être alors gérer une retenue.

4. Propriétés de la multiplication

a. Cela dépend également des nombres sur lesquels on va opérer.

b. $(n)_{CLE} \times (m)_{CLE} = 2^n \times 2^m = 2^{n+m} = (n+m)_{CLE}$.

c. $(5; 2; 0)_{CLE} \times (4)_{CLE} = (2^5 + 2^2 + 2^0) \times (2^4) = 2^{5+4} + 2^{2+4} + 2^{0+4} = (9; 6; 4)_{CLE}$

$(5; 3)_{CLE} \times (7; 2; 1)_{CLE} = (5)_{CLE} \times (7; 2; 1)_{CLE} + (3)_{CLE} \times (7; 2; 1)_{CLE}$
 $= (7 + 5; 2 + 5; 1 + 5)_{CLE} + (7 + 3; 2 + 3; 1 + 3)_{CLE}$
 $= (12; 7; 6)_{CLE} + (10; 5; 4)_{CLE} = (12; 10; 7; 6; 5; 4)_{CLE}$

d. Règle générale pour effectuer le produit de deux nombres CLE

Le produit de deux nombres CLE est constitué de toutes les sommes possibles entre les chiffres de l'un et les chiffres de l'autre des 2 nombres, si une même somme apparaît 2 fois, on passe la retenue en écrivant le suivant.

e. $(12; 4)_{CLE}^2 = (12; 4)_{CLE} \times (12; 4)_{CLE} = (12)_{CLE} \times (12; 4)_{CLE} + (4)_{CLE} \times (12; 4)_{CLE}$
 $= (24; 16)_{CLE} + (16; 8)_{CLE} = (24; 17; 8)_{CLE}$

Exercice 62

Mieux vaut être optimiste et se tromper que pessimiste et avoir raison.

On considère l'entier naturel $n = 19^{88} - 1$.

1.a. Montrer que $n = (19^{11} - 1)(19^{11} + 1)(19^{22} + 1)(19^{44} + 1)$.

b. Montrer que 9 divise $19^{11} - 1$ et que 3 ne divise pas $(19^{11} + 1)(19^{22} + 1)(19^{44} + 1)$.

c. En remarquant que $18 = 2 \times 3^2$, prouver que : $19^{11} - 1 = \sum_{k=1}^{11} C_{11}^k 2^k 3^{2k}$

Montrer que $19^{11} - 1 \equiv 9 [27]$. Quelle est donc la plus grande puissance de 3 qui divise $n = 19^{88} - 1$?

2.a. Prouver que les entiers $19^{11} - 1$, $19^{22} + 1$ et $19^{44} + 1$ sont pairs non divisibles par 4.

b. Prouver que $19^{11} + 1 \equiv 0 [4]$ et que $19^{11} + 1 \not\equiv 0 [8]$.

c. En déduire la plus grande puissance de 2 qui divise $n = 19^{88} - 1$.

3. Calculer la somme des diviseurs de n de la forme $d = 2^a \times 3^b$ avec a, b dans $\mathbb{N}$.

Corrigé

1.a. On a successivement par manipulation des identités remarquables classiques :

$$n = 19^{88} - 1 = (19^{44})^2 - 1^2 = (19^{44} - 1)(19^{44} + 1) = (19^{22} - 1)(19^{22} + 1)(19^{44} + 1)$$

$$= (19^{11} - 1)(19^{11} + 1)(19^{22} + 1)(19^{44} + 1)$$

b. On sait que $19 \equiv 1 [9]$ et donc $19^{11} - 1 \equiv 1^{11} - 1 \equiv 0 [9]$. Ce qui signifie que 9 divise $19^{11} - 1$. D'autre part, on remarque que 3 ne divise pas le produit $(19^{11} + 1)(19^{22} + 1)(19^{44} + 1)$ puisque :

$$19 \equiv 1 [3] \Rightarrow \begin{cases} 19^{11} + 1 \equiv 2 [3] \\ 19^{22} + 1 \equiv 2 [3] \\ 19^{44} + 1 \equiv 2 [3] \end{cases}$$

et aucun des entiers $19^{11} + 1$, $19^{22} + 1$ et $19^{44} + 1$ n'est divisible par 3.

c. On rappelle la formule du développement du binôme de Newton :

$$\forall a, b \text{ de } \mathbb{R} \text{ et } \forall n \text{ entier } \geq 2, (a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}$$

$$\text{Donc par application de cette formule : } 19^{11} = (18 + 1)^{11} = \sum_{k=0}^{11} C_{11}^k 18^k \times 1^{11-k} = \sum_{k=0}^{11} C_{11}^k 2^k 3^{2k}.$$

Le terme obtenu dans la somme pour $k = 0$ étant $C_{11}^0 \times 2^0 \times 3^0 = 1$, alors on peut conclure que :

$$19^{11} - 1 = \sum_{k=0}^{11} C_{11}^k 2^k 3^{2k}$$

Dans cette dernière somme, tous les termes obtenus à partir de $k = 2$ sont divisibles par 27 et donc la somme peut se réduire à la congruence : $19^{11} - 1 \equiv C_{11}^1 \times 2^1 \times 3^2 \equiv 9 [27]$

On peut récapituler les résultats précédents :

$$\begin{cases} 9 = 3^2 \text{ divise } 19^{11} - 1 \\ 3 \text{ ne divise pas le produit } (19^{11} + 1)(19^{22} + 1)(19^{44} + 1) \\ 27 = 3^3 \text{ ne divise pas } 19^{11} - 1 \end{cases}$$

Donc 3^2 est la plus grande puissance de 3 qui divise $n = 19^{11} - 1$.

2.a. Il est tout à fait évident que les nombres $19^{11} - 1$, $19^{22} + 1$ et $19^{44} + 1$ sont pairs car ils sont tous différences ou sommes de nombres impairs.

$$\text{D'autre part, on a : } 19 \equiv -1 [4] \Rightarrow \begin{cases} 19^{11} - 1 \equiv -2 [4] \\ 19^{22} + 1 \equiv 2 [4] \\ 19^{44} + 1 \equiv 2 [4] \end{cases}$$

Donc enfin les nombres $19^{11} - 1$, $19^{22} + 1$ et $19^{44} + 1$ sont pairs mais non divisibles par 4.

b. On a : $19 \equiv -1 [4] \Rightarrow 19^{11} + 1 \equiv 0 [4]$. Donc $19^{11} + 1$ est divisible par 4.

En revanche $19^{11} + 1$ n'est pas divisible par 8 car $19^{11} + 1 \equiv 3^{11} + 1 = 3 \times (3^2)^5 + 1 \equiv 4 [8]$.

c. En récapitulant les résultats de la deuxième question :

$$\begin{cases} \text{les nombres } 19^{11} - 1, 19^{22} + 1 \text{ et } 19^{44} + 1 \text{ sont pairs mais non divisibles par 4} \\ 19^{11} + 1 \text{ est divisible par } 4 = 2^2 \text{ mais non divisible par } 8 = 2^3 \end{cases}$$

on déduit que la plus grande puissance de 2 qui divise $n = 19^{11} - 1$ est $2 \times 2 \times 2 \times 2^2 = 2^5$.

3. On a démontré :

- À la question 1 que la plus grande puissance de 3 qui divise n est 3^2 ;

- À la question 2 que la plus grande puissance de 2 qui divise n est 2^5 .

Comme 2 et 3 sont premiers entre eux, il en est de même de 2^5 et 3^2 et Gauss permet de conclure que $2^5 \times 3^2$ divise n .

Donc les diviseurs de n de la forme $2^a \times 3^b$ sont tels que $0 \leq a \leq 5$ et $0 \leq b \leq 2$ et par suite la somme des diviseurs de n de la forme $2^a \times 3^b$ est donnée par :

$$\sum_{b=0}^2 \sum_{a=0}^5 2^a \times 3^b$$

D'autre part, on sait que :

$$\sum_{b=0}^2 \sum_{a=0}^5 2^a \times 3^b = \left(\sum_{a=0}^5 2^a \right) \left(\sum_{b=0}^2 3^b \right) = (2^6 - 1)(1 + 3 + 3^2) = 819 \text{ (car } a \text{ ne dépend pas de } b)$$

Exercice 63

Le philosophe cherche des solutions aux problèmes et ne trouve que des problèmes sans solution.

Soit $n > 0$ un entier. On note $S(n)$ la somme des chiffres de l'écriture décimale de n . Le but de l'exercice est de savoir s'il existe un entier $n > 0$ tel que $S(n) = 2017$ et $S(n^2) = 2017^2$?

1. Soit $a_1, a_2, \dots, a_m$ m nombres réels.

a. Montrer que :
$$\left(\sum_{s=1}^{s=m} a_s \right)^2 = \sum_{s=1}^{s=m} a_s^2 + 2 \left(\sum_{1 \leq s < t \leq m} a_s a_t \right).$$

b. Prouver qu'il existe $\frac{m(m-1)}{2}$ couples (s, t) d'entiers naturels tels que $1 \leq s < t \leq m$.

2. Pour la recherche d'un entier n qui répond à la question, l'idée est de choisir un nombre n formé uniquement avec des 0 et des 1 suffisamment espacés pour que l'élévation au carré ne fasse pas produire des retenues. Pour ce fait, on pose :

$$n = \sum_{i=1}^{i=201} 10^{2^i}$$

a. En utilisant les deux items de la question 1, montrer que $S(n) = 2017$ et $S(n^2) = 2017^2$.

b. Généralisation

Soit P un entier naturel non nul. Existe-t-il un entier n tel que $S(n) = P$ et $S(n^2) = P^2$?

Corrigé

1.a. Raisonnons par récurrence sur m .

Soit la propriété P_m : « $\forall m \geq 2$, $\left(\sum_{s=1}^{s=m} a_s \right)^2 = \sum_{s=1}^{s=m} a_s^2 + 2 \left(\sum_{1 \leq s < t \leq m} a_s a_t \right)$ ».

→ Initialisation :

Pour $m = 2$, on a : $(a_1 + a_2)^2 = a_1^2 + a_2^2 + 2a_1 a_2$ et donc P_2 est vraie.

→ On suppose qu'il existe un rang m pour lequel P_m est vraie. Montrons que P_{m+1} est vraie.

On a :

$$\left(\sum_{s=1}^{s=m+1} a_s \right)^2 = \left[\left(\sum_{s=1}^{s=m} a_s \right) + a_{m+1} \right]^2 = \left(\sum_{s=1}^{s=m} a_s \right)^2 + a_{m+1}^2 + 2a_{m+1} \left(\sum_{s=1}^{s=m} a_s \right)$$

Or selon l'hypothèse de récurrence, on a :

$$\left(\sum_{s=1}^{s=m} a_s \right)^2 = \sum_{s=1}^{s=m} a_s^2 + 2 \left(\sum_{1 \leq s < t \leq m} a_s a_t \right)$$

Et l'on sait que :

$$\sum_{s=1}^{s=m} a_s^2 + a_{m+1}^2 = \sum_{s=1}^{s=m+1} a_s^2 \quad \text{et} \quad 2 \left(\sum_{1 \leq s < t \leq m} a_s a_t \right) + 2a_{m+1} \left(\sum_{s=1}^{s=m} a_s \right) = 2 \left(\sum_{1 \leq s < t \leq m+1} a_s a_t \right)$$

D'où finalement :

$$\left(\sum_{s=1}^{s=m+1} a_s \right)^2 = \sum_{s=1}^{s=m+1} a_s^2 + 2 \left(\sum_{1 \leq s < t \leq m+1} a_s a_t \right)$$

La propriété est donc vraie pour $m + 1$.

Conclusion : $\forall m \geq 2$, P_m est vraie .

b. Pour déterminer le nombre de couples (s, t) d'entiers naturels tels que $1 \leq s < t \leq m$, il suffit de fixer à chaque fois la valeur de t et déterminer les couples correspondants.

Valeur fixée de t	Valeurs possibles de s	Nombre de couples
2	1	1
3	1, 2	2
4	1, 2, 3	3
...	...	...
m	1, 2, ..., $m-1$	$m-1$

Il y a donc au total $1 + 2 + 3 + \dots + (m-1) = \frac{m(m-1)}{2}$ couples (s, t) d'entiers naturels tels que :
 $1 \leq s < t \leq m$.

2.a. Le nombre donné $n = \sum_{i=1}^{2017} 10^{2^{2i}}$ est la somme de 2017 puissances de 10, distinctes deux à deux, et donc $S(n) = 2017$.

D'autre part, selon la question 1. a, on a : $n^2 = \sum_{i=1}^{2017} 10^{2^{2i+1}} + 2 \left(\sum_{1 \leq i < j \leq 2017} 10^{2^{2i} + 2^{2j}} \right)$.

Les puissances $10^{2^{2i+1}}$ et $10^{2^{2i} + 2^{2j}}$ sont distinctes deux à deux et de ce fait l'écriture de n^2 comporte 2017 chiffres 1, $\frac{2017 \times 2016}{2}$ chiffres 2 et tous les autres chiffres des 0.

Donc : $S(n^2) = 2017 + 2 \times \frac{2017 \times 2016}{2} = 2017^2$.

b. Il suffit de considérer le nombre : $n = \sum_{i=1}^{2017} 10^{2^{2i}}$.

Exercice 64 L'homme courtois évite de poser le pied sur l'ombre de son voisin.

Le critère d'Eisenstein

Soit l'équation (1) d'inconnue rationnelle x : $78x^3 + ux^2 + vx - 14 = 0$, où $u, v \in \mathbb{Z}$.

1. On suppose dans cette question que $\frac{14}{39}$ est solution de l'équation (1).

a. Prouver que les entiers relatifs u et v sont liés par la relation : $14u + 39v = 1129$.

b. Utiliser l'algorithme d'Euclide, en détaillant les diverses étapes du calcul, pour trouver un couple $(x; y)$ d'entiers relatifs vérifiant l'équation suivante : $14x + 39y = 1$.

Vérifier que le couple $(-25; 9)$ est solution de cette équation.

c. En déduire un couple $(u_0; v_0)$ solution particulière de l'équation suivante : $14u + 39v = 1129$.

Donner la solution générale de cette équation.

d. Déterminer, parmi les couples $(u; v)$ solutions, celui pour lequel le nombre u est l'entier naturel le plus petit possible.

2.a. Décomposer 78 et 14 en facteurs premiers. En déduire, dans $\mathbb{N}$, l'ensemble des diviseurs de 78 et l'ensemble des diviseurs de 14.

b. Soit $\frac{P}{Q}$ une solution rationnelle de l'équation (1) d'inconnue x : $78x^3 + ux^2 + vx - 14 = 0$.

Montrer que si P et Q sont des entiers relatifs premiers entre eux, alors P divise 14 et Q divise 78.

On démontre « Critère d'Eisenstein : Si l'équation (E) $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ admet une solution rationnelle irréductible $\frac{P}{Q}$ alors p divise a_0 et q divise a_n . »

c. En déduire le nombre de rationnels, non entiers, pouvant être solutions de l'équation (1) et écrire, parmi ces rationnels, l'ensemble de ceux qui sont positifs.

Corrigé

1.a. On suppose dans cette question que $\frac{14}{39}$ est une solution de l'équation (1).

$$\begin{aligned} \frac{14}{39} \text{ solut. de (1)} &\Leftrightarrow 78 \times \left(\frac{14}{39}\right)^3 + u \left(\frac{14}{39}\right)^2 + v \left(\frac{14}{39}\right) - 14 = 0 \Leftrightarrow 2 \times 39 \times \frac{14^3}{39^3} + u \frac{14^2}{39^2} + v \frac{14}{39} - 14 = 0 \\ &\Leftrightarrow 2 \times \frac{14^3}{39^2} + u \frac{14^2}{39^2} + v \frac{14}{39} - 14 = 0 \Leftrightarrow 2 \times \frac{14^2}{39^2} + u \frac{14}{39^2} + v \frac{1}{39} - 1 = 0 \\ &\Leftrightarrow 2 \times 14^2 + 14u + 39v - 39^2 = 0 \Leftrightarrow 14u + 39v = 39^2 - 2 \times 14^2 = 1129. \end{aligned}$$

b. Utilisons l'algorithme d'Euclide étendu au couple $(14; 39)$

$a \rightarrow$	39	1	0
$b \rightarrow$	14	0	1
$r \rightarrow$	11	1	-2
	3	-1	3
	2	4	-11
	1	-5	14
	0	14	-39

A partir de la 3^{ème} ligne, chaque ligne est construite à l'aide des deux précédentes selon la formule :

$$L_3 = L_1 - qL_2$$

où q est le quotient de a par b . Ainsi, on a :

$$\text{PGCD}(39; 14) = 1$$

et $14 \times 14 + 39 \times (-5) = 1$
(Pour l'explication voir le cours)

Donc le couple $(14; -5)$ est solution de $14x + 39y = 1$.

D'autre part, on a bien : $14 \times (-25) + 39 \times 9 = -350 + 351 = 1$.

Donc le couple $(-25; 9)$ est solution de : $14x + 39y = 1$.

c. Il suffit de multiplier une solution particulière $(x_0; y_0)$ de l'équation $14x + 39y = 1$ par 1129 pour obtenir une solution particulière $(u_0; v_0)$ de l'équation $14u + 39v = 1129$.

Ainsi, les couples $(14 \times 1129; -5 \times 1129) = (15806; -5645)$ et $(-25 \times 1129; 9 \times 1129) = (-28225; 10161)$ sont des solutions particulières de l'équation :

$$14u + 39v = 1129.$$

Résolution de l'équation $14u + 39v = 1129$:

Soit $(u; v)$ une solution quelconque de $14u + 39v = 1129$.

On a : $14u + 39v = 1129$ et $14 \times (-28225) + 39 \times (10161) = 1129$

Donc par différence des deux égalités précédentes, on obtient :

$$14(u + 28225) = -39(v - 10161) \quad (i)$$

On sait que 14 divise $39(v - 10161)$ et $14 \wedge 39 = 1$, donc, d'après le théorème de Gauss, 14 divise $v - 10161$ c'est-à-dire qu'il existe un entier relatif k tel que $v = 14k + 10161$. En remplaçant $v - 10161$ par $14k$ dans (i), on trouve :

$$14(u + 28225) = -39 \times 14k \text{ soit } u = -39k - 28225.$$

Donc l'ensemble des solutions de l'équation $14u + 39v = 1129$ est :

$$S = \{(-39k - 28225; 14k + 10161) \text{ avec } k \text{ entier relatif}\}$$

d. u est un entier naturel signifie que $-39k - 28225 \geq 0$, soit $k \leq -\frac{28225}{39} \cong -723,71$. On prend

$k = -724$ et alors on obtient : $u = 39 \times 724 - 28225 = 11$ et $v = 10161 - 724 \times 14 = 25$.

Le couple solution avec la plus petite valeur entière u est $(u; v) = (11; 25)$.

2.a. On a : $78 = 2 \times 3 \times 13$ et donc $D_{78} = \{1; 2; 3; 6; 13; 26; 39; 78\}$

$$14 = 2 \times 7 \text{ et donc } D_{14} = \{1; 2; 7; 14\}.$$

b. Si P et Q sont solutions de (1) alors $78\left(\frac{P}{Q}\right)^3 + u\left(\frac{P}{Q}\right)^2 + v\left(\frac{P}{Q}\right) - 14 = 0$ c'est-à-dire que :

$$78P^3 + uP^2Q + vPQ^2 - 14Q^3 = 0.$$

En factorisant P on obtient : $P(78P^2 + uQ + vQ^2) = 14Q^3$

En factorisant Q on obtient : $-78P^3 = Q(uP^2 + vPQ - 14Q^2)$

P divise $14Q^3$ or $P \wedge Q = 1$ donc d'après le théorème de Gauss, P divise 14.

Q divise $78P^3$ or $P \wedge Q = 1$ donc d'après le théorème de Gauss, Q divise 78.

c. Comme $P \wedge Q = 1$ donc P et Q ne peuvent être pairs tous les deux (cas grisés).

Voici donc les 20 solutions rationnelles positives possibles de l'équation (1) ; il y en a 20 autres négatives.

$\begin{matrix} P \rightarrow \\ Q \downarrow \end{matrix}$	1	2	3	6	13	26	39	78
1		$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{13}$	$\frac{1}{26}$	$\frac{1}{39}$	$\frac{1}{78}$
2			$\frac{2}{3}$		$\frac{2}{13}$		$\frac{2}{39}$	
7		$\frac{7}{2}$	$\frac{7}{3}$	$\frac{7}{6}$	$\frac{7}{13}$	$\frac{7}{26}$	$\frac{7}{39}$	$\frac{7}{78}$
14			$\frac{14}{3}$		$\frac{14}{13}$		$\frac{14}{39}$	

Exercice 65

Une route peut prendre mille directions, la vérité n'en connaît qu'une...

Soit $(a; b) \in \mathbb{N} \times \mathbb{N}$, $a \geq 2$, $b \geq 2$ tels que $\text{PGCD}(a; b) = 1$.

1. Démontrer qu'il existe deux entiers relatifs non nuls de signes contraires u et v tels que : $au + bv = 1$.

2. Soit $k \in \mathbb{N}$.

a. Démontrer qu'il existe deux relatifs non nuls de signes contraires m_0 et n_0 tels que $am_0 + bn_0 = k$.

b. Démontrer, à l'aide d'une division euclidienne bien choisie, que si $k \geq (a-1)(b-1)$, il existe deux entiers naturels m et n tels que : $am + bn = k$.

3. Application : Sur une planète lointaine, les habitants ne disposent que de pièces de 5 et 8 bitni. Le client d'un restaurant doit régler une note de x bitni, $x > 0$. Établir suivant les valeurs de l'entier x si le client peut régler exactement la note ou non dans les deux cas suivants :

a. On suppose que client de réserves et restaurateur disposent de réserves inépuisables de pièces de 5 et 8 bitni pour payer et rendre la monnaie.

b. On suppose que le client dispose de réserves inépuisables de pièces de 5 et 8 bitni, mais que la caisse du restaurateur est vide.

Corrigé

1. On a $\text{PGCD}(a; b) = 1$, donc d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que :

$$au + bv = 1.$$

Démontrons par l'absurde que u et v sont non nuls.

→ Si $u = v = 0$, alors $0 + 0 = 1$, ce qui est absurde.

→ Si $u = 0$, alors $v \neq 0$ et $|bv| = b \times |v| \geq 2|v| \geq 2$, ce qui est absurde car $bv = 1$.

→ De même, $v \neq 0$ car $a \geq 2$.

Donc $u \neq 0$ et $v \neq 0$.

Démontrons par l'absurde que u et v sont de signes contraires : supposons que u et v soient de même signe.

→ Si $u > 0$ et $v > 0$, alors $u \geq 1$ et $v \geq 1$. Or $a \geq 2, b \geq 2$, donc $au + bv \geq 4$, ce qui est absurde.

→ Si $u < 0$ et $v < 0$, alors $u \leq -1$ et $v \leq -1$. Or $a \geq 2, b \geq 2$, donc $au + bv \leq -4$, ce qui est absurde.

Donc u et v sont de signes contraires.

2.a. Si $k = 0, m_0 = b$ et $n_0 = -a$ conviennent.

Si $k > 0$, d'après 1., $au + bv = 1$ avec u et v entiers relatifs non nuls et de signes contraires.

On pose $m_0 = ku, n_0 = kv$, et on a : $am_0 + bn_0 = k$.

On en déduit $m_0 \in \mathbb{Z}^*, n_0 \in \mathbb{Z}^*$, et m_0 a même signe que u, n_0 a même signe que v .

Ainsi m_0 et n_0 sont des entiers relatifs non nuls, de signes contraires, tels que $am_0 + bn_0 = k$.

b. On suppose $k \geq (a-1)(b-1) \geq 1$.

On a $am_0 + bn_0 = k$ avec m_0 et n_0 des entiers relatifs non nuls, de signes contraires. On a donc $m_0 > 0$ et $n_0 < 0$ ou $m_0 < 0$ et $n_0 > 0$.

→ Supposons qu'on ait $m_0 > 0$, donc $n_0 < 0$. On effectue alors la division euclidienne de m_0 par b :

Il existe $q \in \mathbb{Z}, r \in \mathbb{N}, 0 \leq r < b$, tels que $m_0 = bq + r$. Alors $a(bq + r) + bn_0 = k$. Donc $ar + b(aq + n_0) = k$.

On pose alors $m = r$ et $n = aq + n_0$. Donc $m \in \mathbb{N}$ et $n \in \mathbb{Z}$.

Montrons par l'absurde que $n \in \mathbb{N}$: supposons $n < 0$. Alors $n \leq -1, b > 0$, donc $bn \leq -b$.

De plus, $m = r \leq b-1$ et $a > 0$, donc $am \leq a(b-1)$.

Ainsi $am + bn \leq a(b-1) - b < a(b-1) - b + 1$, soit $am + bn \leq (a-1)(b-1)$, ce qui est absurde car $am + bn = k \geq (a-1)(b-1)$. On en déduit que $n \in \mathbb{N}$.

→ Supposons qu'on ait $m_0 < 0$ et $n_0 > 0$.

On effectue cette fois la division euclidienne de n_0 par a . Le même raisonnement permet de trouver deux entiers naturels m et n tels que $am + bn = k$.

3.a. Soit $x > 0$ le montant de la note à payer.

Pour pouvoir être réglée, cette facture doit pouvoir s'écrire : $x = 5u + 8v$, avec $(u; v) \in \mathbb{Z}^2$, positifs quand il s'agit de pièces données par le client, négatifs quand il s'agit de pièces rendues par le restaurateur. x doit donc être un entier strictement positif : $x \in \mathbb{N}^*$.

Réciproquement, soit $x \in \mathbb{N}^*$.

On a $\text{PGCD}(5; 8) = 1$, donc d'après 2.a., il existe $m \in \mathbb{Z}^*, n \in \mathbb{Z}^*$ tels que $5m + 8n = x$.

La facture peut donc être réglée si, et seulement si, $x \in \mathbb{N}^*$.

b. Cette fois-ci, la facture peut être réglée si, et seulement si, x peut s'écrire $x = 5u + 8v$, avec $u \in \mathbb{N}$, et $v \in \mathbb{N}$. On doit donc à nouveau avoir $x \in \mathbb{N}^*$.

Comme $\text{PGCD}(5; 8) = 1$, d'après 2.b. appliqué à $a = 5$ et $b = 8$, pour tout $x \in \mathbb{N}^*$ tel que $x \geq 4 \times 7 = 28$, il existe $(m; n) \in \mathbb{Z}^2$ tels que $x = 5m + 8n$.

Reste à traiter les cas où $x \in \mathbb{N}^*, x \leq 28$. On sait que $x = 5u + 8v$ avec $(u; v) \in \mathbb{N}^2$ si, et seulement si :

$$\begin{aligned} &\begin{cases} u = 0 \\ v = 1 \text{ ou } v = 2 \text{ ou } v = 3 \end{cases} \quad \text{ou} \quad \begin{cases} v = 0 \\ u = 1 \text{ ou } u = 2 \text{ ou } u = 3 \text{ ou } u = 4 \text{ ou } u = 5 \end{cases} \\ &\quad \text{ou} \quad \begin{cases} u = 1 \\ v = 1 \text{ ou } v = 2 \end{cases} \quad \text{ou} \quad \begin{cases} u = 2 \\ v = 1 \text{ ou } v = 2 \end{cases} \quad \text{ou} \quad \begin{cases} u = 3 \\ v = 1 \end{cases} \end{aligned}$$

donc si, et seulement si : $x \in \{5; 8; 10; 13; 15; 16; 18; 20; 21; 23; 24; 25; 26\}$.

La facture peut donc être payée si, et seulement si :

$$x \in \{5; 8; 10; 13; 15; 16; 18; 20; 21; 23; 24; 25; 26; k \text{ avec } k \geq 28\}$$

Exercice 66

La guerre, c'est la guerre des hommes ; la paix c'est la guerre des idées.

Un astronome a observé au jour J_0 le corps céleste A , qui apparaît périodiquement tous les 105 jours. Six jours plus tard ($J_0 + 6$), il observe le corps B , dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome. Le but de cet exercice est de déterminer la date de ce jour J_1 .

1. Soient u et v le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1 . Montrer que le couple $(u; v)$ est solution de l'équation $E_1 : 35x - 27y = 2$.

2.a. Déterminer un couple d'entiers relatifs $(x_0; y_0)$ solution particulière de $E_2 : 35x - 27y = 1$.

b. En déduire une solution particulière $(u_0; v_0)$ de E_1 .

c. Déterminer toutes les solutions de l'équation E_1 .

d. Déterminer la solution $(u; v)$ permettant de déterminer J_1 ?

3.a. Combien de jours s'écouleront entre J_0 et J_1 ?

b. Le jour J_0 était le mardi 7 décembre 1999, quelle est la date exacte du jour J_1 ? (l'année 2000 était bissextile).

c. Si l'astronome manque ce futur rendez-vous, combien de jours devra-t-il attendre jusqu'à la prochaine conjonction des deux astres ?

Corrigé

1. Soit u et v les nombres de périodes effectuées par A entre J_0 et J_1 , et par B entre $J_0 + 6$ et J_1 respectivement; alors le nombre de jours écoulés pour A est $105u$, qui est le même que celui vu par B qui s'écrit $6 + 81v$. On a donc $105u = 6 + 81v$, soit $35u - 27v = 2$; donc (u, v) est solution de l'équation E_1 .

2.a. Pour une solution particulière, on utilise le processus d'Euclide :

$$35 = 27(1) + 8; \quad 27 = 8(3) + 3; \quad 8 = 3(2) + 2; \quad 3 = 2(1) + 1$$

puis on écrit les restes successifs dans un parcours de retour:

$$\begin{aligned} 1 &= 3 - 2 = 27 - 8(3) - (8 - 3 \times 2) = 27 - 8(4) + 3(2) = 27 - (35 - 27) \times 4 + (27 - 8(3)) \times 2 \\ &= 27(1 + 4 + 2) - 35(4) - (35 - 27) \times 6 = 27(7 + 6) - 35(10) = 27(13) - 35(10) \end{aligned}$$

Donc une solution particulière est $(-10; -13)$ pour E_2 .

b. Ayant $35(-10) - 27(-13) = 1$, on déduit $35(-10) \times 2 - 27(-13) \times 2 = 2$, soit :

$$35(-20) - 27(-26) = 2 \text{ et une solution particulière de } E_1 \text{ est : } (-20; -26).$$

c. $E_1 \Leftrightarrow 35x - 27y = 35(-20) - 27(-26) \Leftrightarrow 35(x + 20) = 27(y + 26)$. Donc 35 divise $27(y + 26)$, et comme 35 est premier avec 27 alors 35 divise $y + 26$ (théorème de Gauss); on peut écrire : $y + 26 = 35k$ ($k \in \mathbb{Z}$); alors $35(x + 20) = 27(35k)$ et $x + 20 = 27k$. Réciproquement, $(27k - 20; 35k - 26)$ est solution de E_1 car $35(27k - 20) - 27(35k - 26) = 2$.

d. J_1 est le jour de la première rencontre (ou conjonction) et (u, v) est solution de E_1 ; donc u et v sont les plus petits entiers naturels formant une solution; soit $k = 1$ et $(u, v) = (7, 9)$.

3.a. $J_1 - J_0$ est le temps écoulé pour A avant la première conjonction, et $J_1 - J_0 = 105u$.

Donc $J_1 - J_0 = 105 \times 7$; ainsi 735 jours s'écouleront entre J_0 et J_1 .

b. D'abord, puisque J_0 est un mardi et $735 \equiv 0 \pmod{7}$ alors J_1 est aussi un mardi. Ensuite, $735 = 365 + 366 + 4$ signifie que 2 années et 4 jours s'écouleront: on est au 11 décembre 2001: la date du jour J_1 est mardi 11 décembre 2001.

c. Soit J_2 le jour de la prochaine conjonction; $J_2 - J_1$ est multiple de 105 (nombre de jours écoulés pour A) et aussi $J_2 - J_1$ est multiple de 81 (nombre de jours écoulés pour B). Donc $J_2 - J_1$ est multiple commun de 105 et 81; le plus petit de ces multiples communs est :

$$\text{PPCM}(105, 81) = \text{PPCM}(3 \times 5 \times 7; 3^4) = 3 \times 5 \times 7 \times (2 \times 17) = 3\,570.$$

Donc la conjonction aura lieu après une attente de $3\,570 - 735 = 2\,835$ jours.

Exercice 67**L'argent est plus éloquent que douze membres du parlement.**

On se propose de déterminer les couples d'entiers naturels non nuls vérifiant la relation (F):

$$7^n - 3 \times 2^m = 1.$$

1. On suppose $m \leq 4$. Montrer qu'il y a exactement deux couples solutions.
2. On suppose maintenant $m \geq 5$.
 - a. Montrer que si le couple $(n; m)$ vérifie la relation (F), alors : $7^n \equiv 1 [32]$
 - b. En étudiant les restes de la division euclidienne par 32 des puissances de 7, montrer que si le couple d'entiers $(n; m)$ vérifie (F), alors n est divisible par 4.
 - c. En déduire que si le couple $(n; m)$ vérifie la relation (F), alors : $7^n \equiv 1 [5]$
 - d. Pour $m \geq 5$, existe-t-il des couples $(n; m)$ d'entiers naturels non nuls vérifiant la relation (F) ? (raisonner par l'absurde) (indication: on pourra étudier et utiliser les restes de la division par 5 des puissances de 2)
3. Déterminer l'ensemble des couples de naturels non nuls vérifiant la relation (F).

Corrigé

1. On suppose $m \leq 4$.

Si $m = 1$ la relation (F) s'écrit : $7^n - 6 = 1 \Leftrightarrow 7^n = 7 \Leftrightarrow n = 1$ donc $(1; 1)$ est un couple solution.

Si $m = 2$ la relation (F) s'écrit : $7^n - 12 = 1 \Leftrightarrow 7^n = 13$ (impossible dans $\mathbb{N}$)

Si $m = 3$ la relation (F) s'écrit : $7^n - 24 = 1 \Leftrightarrow 7^n = 25$ (impossible dans $\mathbb{N}$)

Si $m = 4$ la relation (F) s'écrit : $7^n - 48 = 1 \Leftrightarrow 7^n = 49 \Leftrightarrow n = 2$ donc $(2; 4)$ est un couple solution

2. On suppose $m \geq 5$;

- a. Comme $m \geq 5$ on peut écrire $m = 5 + k$ avec $k \in \mathbb{N}$. Ainsi la relation (F) devient :

$$7^n - 3 \times 2^{5+k} = 1 \text{ soit } 7^n - 3 \times 2^5 \times 2^k = 1 \text{ et donc } 7^n = 3 \times 32 \times 2^k + 1 \text{ d'où : } 7^n \equiv 1 [32]$$

- b. $7^4 = 2401 = 75 \times 32 + 1$ donc $7^4 \equiv 1 [32]$ et on en déduit que, pour tout entier $k \in \mathbb{N}$,

$7^{4k} \equiv 1^k \equiv 1 [32]$ puis que $7^{4k+1} \equiv 7 [32]$ puis $7^{4k+2} \equiv 49 \equiv 17 [32]$ et enfin $7^{4k+3} \equiv 23 [32]$ Or, dans la division euclidienne de l'entier n par 4, le reste est soit 0, soit 1, soit 2, soit 3, ce qui signifie que n s'écrit $4k$ ou $4k+1$ ou $4k+2$ ou $4k+3$ avec $k \in \mathbb{N}$.

D'après ce qui précède, on peut affirmer que : $7^n \equiv 1 [32] \Leftrightarrow n = 4k$ avec $k \in \mathbb{N} \Leftrightarrow 4$ divise n .

Or on a démontré au 2.a. que $7^n \equiv 1 [32]$ donc on peut en déduire que 4 divise n .

- c. $7^4 = 2401 = 480 \times 5 + 1$ donc $7^4 \equiv 1 [5]$ et on en déduit que, pour tout entier $k \in \mathbb{N}$:

$$7^{4k} \equiv 1^k = 1 [5].$$

Or on vient de prouver que 4 divise n ; ainsi $n = 4k$ avec $k \in \mathbb{N}$ et de ce fait on peut affirmer que :

$$7^n \equiv 1 [5]$$

- d. Comme $7^n - 3 \times 2^m = 1$, en passant modulo 5 dans chaque membre on obtient : $1 - 3 \times 2^m \equiv 1 [5]$

Donc $-3 \times 2^m \equiv 0 [5]$ c'est-à-dire $3 \times 2^m \equiv 0 [5]$. De plus $2^4 = 16 = 15 + 1$ donc $2^4 \equiv 1 [5]$. On en déduit que, pour tout k entier naturel : $2^{4k} \equiv 1 [5]$ puis $2^{4k+1} \equiv 2 [5]$ puis $2^{4k+2} \equiv 4 [5]$ et enfin $2^{4k+3} \equiv 3 [5]$

Ainsi, par disjonction des cas modulo 4:

$Si n \equiv \dots [4]$	0	1	2	3
Alors $2^n \equiv \dots [5]$	1	2	4	3
Donc $3 \times 2^n \equiv \dots [5]$	3	1	2	4

On constate que, dans aucun cas on a $3 \times 2^m \equiv 0 [5]$. Donc il n'existe aucun couple d'entiers non nuls vérifiant la relation (F) dès que $m \geq 5$.

3. On en conclut que $S = \{(1; 1), (2; 4)\}$.

Exercice 68**La distance qui relie la terre au ciel est celle de la pensée.**

1. Déterminer :

- a. le nombre de multiples de 13 compris entre 1 et 10 000 ;
- b. Le nombre de multiples de 13^2 compris entre 1 et 10 000 ;

- c. le nombre de multiples de 13^3 compris entre 1 et 10 000.
2. Existe-t-il des multiples 13^4 compris entre 1 et 10 000.
3. Montrer que le nombre 10 000! est divisible par 13^{832} .
4. a. Déterminer par combien de zéros se termine $100!$
b. En déduire par combien de zéros se termine $127!$

Corrigé

1.a. Il s'agit de déterminer le plus grand entier k tel que $1 \leq 13^k \leq 10\,000$.

On trouve $1 \leq k \leq 769$. Donc il existe 769 multiples de 13 compris entre 1 et 10 000.

b. On a : $1 \leq 13^2 k \leq 10\,000 \Rightarrow 1 \leq k \leq 59$. Donc, il y a 59 multiples de 13^2 entre 1 et 10 000.

c. On a : $1 \leq 13^3 k \leq 10\,000 \Rightarrow 1 \leq k \leq 4$. Donc, il y a 4 multiples de 13^3 compris entre 1 et 10 000.

2. comme $13^4 = 28\,561 > 10\,000$, il n'existe aucun multiple de 13^4 compris entre 1 et 10 000.

3. D'après la question précédente, on peut dire :

→ qu'il existe $769 - 59 = 710$ multiples de 13, compris entre 1 et 10 000, qui ne sont pas des multiples de 13^2 ;

→ qu'il existe $59 - 4 = 55$ multiples de 13^2 , compris entre 1 et 10 000, qui ne sont pas des multiples de 13^3 .

Donc on peut conclure qu'il existe un entier Q tel que :

$$\begin{aligned} 10\,000! &= \underbrace{13 \times 13 \times \dots \times 13}_{710 \text{ fois}} \times \underbrace{13^2 \times 13^2 \times \dots \times 13^2}_{55 \text{ fois}} \times \underbrace{13^3 \times \dots \times 13^3}_{4 \text{ fois}} \times Q \\ &= 13^{710} \times (13^2)^{55} \times (13^3)^4 \times Q = 13^{710+110+12} \times Q = 13^{832} \times Q \end{aligned}$$

Donc 10 000! est divisible par 13^{832} .

4.a. On rappelle que si un entier x s'écrit $x = a \times 10^p$ tel que $a \not\equiv 0 [10]$ et $p \in \mathbb{N}^*$ alors l'écriture décimale de a se termine par p chiffres « 0 ». Dans cette question, il s'agit de déterminer les exposants respectifs m et n de 2 et 5 dans la décomposition en facteurs premiers de $100!$ (m est appelé la valuation 2 – adique de $100!$ et n sa valuation 5 – adique). Si on arrive à « épuiser » les facteurs premiers 2 et 5 dans $100!$, on pourra ainsi écrire $100! = 10^{\min(m,n)} \times Q$ où $Q \not\equiv 0 [10]$ et dans ce cas $100!$ se termine par $p = \min(m; n)$ chiffres « 0 ». Ici, il appert de toute évidence que $p = \min(m; n) = n$ car il y a plus de multiples de 2 que de 5 entre 1 et 100. De ce fait, nous pouvons nous limiter à déterminer seulement la valuation 5 – adique de $100!$.

On voit clairement :

- qu'il existe 20 multiples de 5 compris entre 1 et 100 ;
- qu'il existe 4 multiples de 5^2 compris entre 1 et 100 ;
- qu'il n'existe aucun multiple de 5^3 entre 1 et 100.

D'autre part, entre 1 et 100, il y a 16 ($= 20 - 4$) multiples de 5 qui ne sont pas des multiples de 5^2 .

$$\begin{aligned} \text{D'où : } 100! &= 2^m \times \underbrace{5 \times 5 \times \dots \times 5}_{16 \text{ fois}} \times \underbrace{5^2 \times 5^2 \times 5^2 \times 5^2}_{4 \text{ fois}} \times Q = 2^m \times 5^{24} \times Q \\ &= 2^{24} \times 5^{24} \times 2^{m-24} \times Q = 10^{24} \times 2^{m-24} \times Q. \end{aligned}$$

Donc l'écriture décimale de $100!$ se termine par 24 zéros.

b. On sait que $127! = 100! \times 101 \times 102 \times \dots \times 127$ et que entre 101 et 127, on peut facilement compter les multiples de 5 (ceux de 2 sont à « gogo »). Ainsi :

$$105 = \boxed{5} \times 21 ;$$

$$110 = \boxed{5} \times 22 ;$$

$$115 = \boxed{5} \times 23 ;$$

$$120 = \boxed{5} \times 24 ;$$

$$125 = \boxed{5} \times \boxed{5} \times \boxed{5}.$$

Donc, il y a sept nouveaux facteurs tous égaux à 5 et par suite $127!$ se termine par 31 ($= 24 + 7$) zéros.

Exercice 69

Tu as une langue et deux oreilles: dis un seul mot pour en écouter deux.

une infinité de nombres amis

On peut vérifier facilement que les entiers 30 et 140 sont amis, c'est-à-dire que leur quotient est égal au quotient de la somme de tous leurs diviseurs positifs. On dit que les nombres 30 et 140 **sont amis**.

1. Soit a un entier naturel supérieur ou égal à 2 et p un entier premier qui ne divise pas a .
 - a. Montrer que le nombre de diviseurs du produit $p \times a$ est le double du nombre de diviseurs de a .
 - b. On note $d_1, d_2, \dots, d_m$ la liste des diviseurs de a . Ecrire la liste des diviseurs de $p \times a$.
 - c. En notant S la somme des diviseurs positifs d'un entier $n \geq 2$, montrer que : $S_{pa} = (1 + p)S_a$.
2. Dédurre de la question 1 la propriété suivante : « Si a et b sont amis et si p est nombre premier ne divisant ni a ni b alors les nombres $p \times a$ et $p \times b$ sont amis ».
3. Avec cette propriété et une paire d'amis connue, on peut créer une infinité de paires d'amis.
 - a. Justifier l'affirmation ci-dessus.
 - b. Proposer trois paires d'amis engendrées par la paire $\{30; 140\}$.

Corrigé

- 1.a. Soit la décomposition en facteurs premiers : $a = q_1^{\alpha_1} \times q_2^{\alpha_2} \times \dots \times q_k^{\alpha_k}$. Le nombre pa admet comme décomposition en facteurs premiers : $p \times q_1^{\alpha_1} \times q_2^{\alpha_2} \times \dots \times q_k^{\alpha_k}$ où p est distinct de tous les q_i .
Si on appelle N le nombre de diviseurs de a le nombre de diviseurs de Pa est égal à $(1 + 1)N = 2N$.
- b. Les diviseurs de Pa sont $d_1; \dots; d_m; pd_1; \dots; pd_m$.
- c. $S_{pa} = d_1 + d_2 + \dots + d_m + pd_1 + pd_2 + \dots + pd_m = S_a + pS_a = (1 + p)S_a$.
2. Si a et b sont amis, alors $\frac{a}{b} = \frac{S_a}{S_b}$; Or $S_{pa} = (1 + p)S_a$ et $S_{pb} = (1 + p)S_b$, donc :

$$\frac{pa}{pb} = \frac{a}{b} = \frac{S_a}{S_b} = \frac{S_{pa}}{S_{pb}}$$

et donc pa et pb sont amis.

- 3.a. Il suffit de multiplier les deux nombres amis par un nombre premier p qui n'intervient dans aucune décomposition en facteurs premiers des deux nombres. Comme les facteurs premiers communs sont en nombre fini et qu'il y a une infinité de nombres premiers, il y a une infinité de choix possibles pour p .
- b. $\{11 \times 30; 11 \times 140\}; \{13 \times 30; 13 \times 140\}; \{17 \times 30; 17 \times 140\}$ sont des paires de nombres amis.

Exercice 70

Le mensonge te rend service un jour, la vérité toujours.

Les nombres amiables de Thabit ibn Qurra

1. Établir la liste des diviseurs positifs propres de 284 et calculer leur somme notée S_{284} .
2. Reprendre la question avec le nombre 220. On remarque que chacun de ces deux nombres est la somme des diviseurs positifs propres de l'autre. On dit que 284 et 220 sont des nombres **amiables** (ou **amicaux** ou **aimables**).

Pour tout entier naturel non nul n , on pose :

$$a = 3 \times 2^{n-1} - 1; b = 3 \times 2^n - 1; c = 9 \times 2^{2n-1} - 1; A = 2^n \times a \times b; B = 2^n \times c.$$

Le savant arabe Thabit ibn Qurra a démontré que : « Si a , b et c sont premiers, alors A et B sont amiables ».

- 3.a. Vérifier que les nombres 220 et 284 sont de la forme de A et B .

Cette paire de nombres amiables était connue de Pythagore au VI^e siècle av. J.-C.

- b. Montrer que 1 184 et 1 210 sont amiables.

Cette paire d'amiables, pourtant formée de nombres assez petits, n'a été proposée qu'en 1867 par un jeune amateur italien Nicolo Paganini.

- c. Calculer a , b et c pour $n = 4$ et vérifier qu'ils sont premiers. Calculer la paire de nombres amiables A et B obtenue. Cette paire a été donnée par Fermat au XVII^e siècle.

- d. Même question avec $n = 7$. Cette paire d'amiables a été donnée par Descartes en 1638.

4. Démonstration de la propriété. (Tous les diviseurs considérés sont positifs) On suppose que a , b et c sont premiers. Comme a et b sont distincts, les écritures $A = 2^n \times a \times b$ et $B = 2^n \times c$ sont les décompositions en facteurs premiers des entiers A et B .

- a. Justifier que les entiers $1; 2; \dots; 2^n; c; c \times 2; \dots, c \times 2^n$ sont les seuls diviseurs de B .

- b. Établir de même la liste des diviseurs de A .

- c. Montrer que la somme S_B des diviseurs de B est égal à $(1 + c)(2^{n+1} - 1)$.

- d. Montrer que la somme S_A des diviseurs de A est égale à : $(1 + a + b + ab)(2^{n+1} - 1)$.

- e. En utilisant les expressions de a , b et c en fonction de n , montrer que $S_A = S_B$ et conclure.

Corrigé (N.B : Les diviseurs propres positifs d'un entier sont ses diviseurs dans $\mathbb{N}$ hormis lui-même.)

1. On a : $220 = 2^2 \times 5 \times 11$, d'où : $\text{Div}_{\mathbb{N}}(220) = \{1; 2; 4; 5; 10; 11; 20; 22; 44; 55; 110; 220\}$ et donc :
 $S_{220} = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$

2. On a : $284 = 2^2 \times 71$ d'où $\text{Div}_{\mathbb{N}}(284) = \{1; 2; 4; 71; 142; 284\}$ et donc :
 $S_{284} = 1 + 2 + 4 + 71 + 142 = 220$.

Donc 220 et 284 sont des nombres amiables.

3. a. $220 = 2^2 \times 5 \times 11$ et $284 = 2^2 \times 71$ sont de la forme A et B avec $n = 2$.

b. Les diviseurs propres positifs de 184 sont 1; 2; 4; 8; 16; 32; 37; 74; 148; 296; 592; et leur somme est : 1 210. Les diviseurs propres positifs de 1 210 sont 1; 2; 5; 10; 11; 22; 55; 110; 121; 242; 605; et leur somme est 1 184. Donc 1 184 et 1 210 sont amiables.

On a : $1184 = 2^5 \times 37$ et $1210 = 2 \times 5 \times 11^2$, donc ils ne sont pas de la forme A et B.

c. Pour $n = 4$, on a $a = 23$; $b = 47$; $c = 1151$ qui sont premiers et donnent la paire suivante de nombres amiables $A = 17\,296$; $B = 18\,416$.

d. Pour $n = 7$, on a $a = 191$; $b = 383$; $c = 73\,727$ qui sont premiers et donnent la paire suivante de nombres amiables $A = 9\,363\,584$; $B = 9\,437\,056$.

4 a. Il y a $2(n + 1)$ diviseurs positifs de B et les diviseurs proposés sont distincts et au nombre de $2(n + 1)$.

b. A possède $(n + 1) \times 2 \times 2 = 4(n + 1)$ diviseurs positifs; ce sont les entiers:

$$1; 2; 2^2; \dots; 2^n; a; 2a; 2^2a; \dots; 2^na; b; 2b; 2^2b; \dots; 2^nb; ab; 2ab; 2^2ab; \dots; 2^nab.$$

$$c. S_B = (1 + 2 + 2^2 + \dots + 2^n)(1 + c) = \frac{1-2^{n+1}}{1-2}(1 + c) = (2^{n+1} - 1)(1 + c)$$

$$d. S_A = (1 + 2 + 2^2 + \dots + 2^n)(1 + a + b + ab) = (2^{n+1} - 1)(1 + a + b + ab)$$

$$e. 1 + a + b + ab = 1 + 3 \times 2^{n-1} - 1 + 3 \times 2^n - 1 + (3 \times 2^{n-1} - 1)(3 \times 2^n - 1) \\ = 3 \times 2^{n-1} + 3 \times 2^n - 1 + 9 \times 2^{2n-1} - 3 \times 2^{n-1} - 3 \times 2^n + 1 = 9 \times 2^{2n-1} = c + 1.$$

Ainsi, $S_A = S_B$ et A et B sont amiables.

Exercice 71

Le riche avare est semblable à un âne chargé d'or, qui mange de la paille.

1. Cette question est purement une question de cours

a. Soient a, b, c et d des entiers relatifs. Démontrer que :

$$\text{Si } a \equiv b [7] \text{ et } c \equiv d [7] \text{ alors } a \times c \equiv b \times d [7].$$

b. En déduire que pour a et b relatifs non nuls si $a \equiv b [7]$ alors pour tout naturel n , on a : $a^n \equiv b^n [7]$.

2. Pour $a = 2$ puis pour $a = 3$, déterminer un entier naturel n non nul tel que : $a^n \equiv 1 [7]$.

3. Soit a un entier naturel non divisible par 7.

a. Montrer que : $a^6 \equiv 1 [7]$.

b. On appelle ordre de a modulo 7 le plus petit naturel k non nul tel que $a^k \equiv 1 [7]$. Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1 [7]$. En déduire que k divise 6. Quelles sont les valeurs possibles de l'entier k ?

c. Donner l'ordre modulo 7 de tous les entiers naturels a compris entre 2 et 6.

4. A tout naturel n , on associe le nombre A_n défini par : $A_n = 2^n + 3^n + 4^n + 5^n + 6^n$.

Montrer que $A_{2006} \equiv 6 [7]$.

Corrigé

1. a. En écrivant $a = b + 7k$, $c = d + 7k'$ on trouve que :

$$ac = (b + 7k)(d + 7k') = bd + 7(bk' + dk + kk') \text{ et donc : } ac \equiv bd [7]$$

b. Récurrence:

Soit (P_n) la propriété: « $\forall n \in \mathbb{N}, a^n \equiv b^n [7]$ »

• Initialisation :

(P_0) est vraie car $1 \equiv 1 [7]$

(P_1) est vraie d'après la question précédente.

• Hérédité : supposons qu'il existe un rang p pour lequel (P_p) est vraie c'est-à-dire que $a^p \equiv b^p [7]$ et montrons que (P_{p+1}) est vraie. On a $a \equiv b [7]$ et par hypothèse de récurrence : $a^p \equiv b^p [7]$. Donc en appliquant les résultats de la question 1.a. on trouve : $a^p \times a \equiv b^p \times b [7]$ i.e $a^{p+1} \equiv b^{p+1} [7]$ et donc (P_{p+1}) est vraie.

Conclusion : (P_0) est vraie et (P_n) est héréditaire à partir de $n = 0$ donc la propriété est générale.

2. Pour $a = 2$ puis pour $a = 3$, déterminer un naturel n non nul minimal tel que $a^n \equiv 1 [7]$. On cherche les restes de 2^n et 3^n dans la division par 7 :

$n \equiv \dots [7]$	1	2	3	4	5	6
$2^n \equiv \dots [7]$	2	4	1	2	4	1
$3^n \equiv \dots [7]$	3	2	6	4	5	1

Donc pour $a = 2$, on trouve $n = 3$ et pour $a = 3$, on trouve $n = 6$.

3.a. Le petit théorème de Fermat dit que si p est un entier premier ne divisant pas a , alors $a^{p-1} \equiv 1 [p]$. Dans notre cas, a est un entier non divisible par l'entier $p = 7$. Donc : $a^6 \equiv 1 [7]$.

b. En divisant 6 par k , on peut écrire $6 = kq + r$ et $0 \leq r < k$, on a :

$6 = kq + r \Rightarrow a^6 = a^{kq} \times a^r = (a^k)^q \times a^r$ et comme $a^k \equiv 1 [7]$ alors on a : $a^r \equiv 1 [7]$. Ce dernier résultat jumelé à la double inégalité $0 \leq r < k$ contredit le caractère de minimalité de k . Donc $r = 0$ et par suite k divise 6, soit $k \in \{1, 2, 3, 6\}$.

c. Pour déterminer l'ordre modulo 7 de chacun des entiers de 2 à 6, on dresse le tableau de congruences suivant :

		$a^2 \equiv \dots [7]$	$a^3 \equiv \dots [7]$	$a^6 \equiv \dots [7]$
$a =$	2 ($k = 3$)	4	1	1
	3 ($k = 6$)	2	6	1
	4 ($k = 3$)	2	1	1
	5 ($k = 6$)	4	6	1
	6 ($k = 2$)	1	6	1

Donc en modulo 7 : $\text{Ord}(2) = 3$, $\text{Ord}(3) = 6$, $\text{Ord}(4) = 3$, $\text{Ord}(5) = 6$ et $\text{Ord}(6) = 2$.

4. On a : $A_{2006} = 2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006}$.

Or $2006 = 2 \times 1003 = 3 \times 668 + 2 = 6 \times 334 + 2$ et par suite compte tenu des ordres modulo 7 des entiers 2, 3, 4, 5 et 6, on trouve :

$$2^{2006} = (2^3)^{668} \times 2^2 \equiv 4 [7] ; 3^{2006} = (3^6)^{334} \times 3^2 \equiv 2 [7] ;$$

$$4^{2006} = (4^3)^{668} \times 4^2 \equiv 2 [7] ; 5^{2006} = (5^6)^{334} \times 5^2 \equiv 4 [7] ;$$

$$6^{2006} = (6^2)^{1003} \equiv 1 [7] .$$

d'où : $A_{2006} = 2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006} \equiv 4 + 2 + 2 + 4 + 1 [7]$, soit en conclusion :

$$A_{2006} \equiv 6 [7] \text{ car } 13 \equiv 6 [7].$$

Exercice 72

Celui qui enseigne le bien aux autres, sans le faire, est semblable à l'aveugle qui porterait une lanterne.

1.a. Le nombre $6n + 15$ est-il premier pour tout entier naturel n ?

b. Le nombre $6n + 5$ est-il premier pour tout entier naturel n ?

2. Le nombre $n^2 + n + 41$ est-il premier pour tout entier naturel n ?

3. On considère le polynôme défini pour x réel par : $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ où $a_0, a_1, \dots, a_n$ sont des entiers relatifs.

a. Supposons que pour un entier m , $P(m)$ soit égal à un nombre premier p . Montrer qu'il existe au moins un entier k pour lequel $P(m + kp)$ est un nombre composé.

b. Est-il possible de trouver un polynôme à coefficients entiers qui ne prenne que des valeurs premières, pour toute valeur entière de la variable ?

Corrigé

1.a. $6n + 15 = 3(2n + 5)$ est toujours composé comme multiple de 3.

b. Faux : $6n + 5$ n'est pas premier pour tout n : pour $n = 5$, il vaut $35 = 5 \times 7$.

2. $n^2 + n + 41$ n'est sûrement pas premier pour $n = 41$ (il est alors clairement divisible par 41).

Ceci étant, cette expression donne un nombre premier pour n allant de 0 jusqu'à 39 inclus.

3. On considère le polynôme non constant défini pour x réel par : $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ où $a_0, a_1, \dots, a_n$ sont des entiers relatifs.

a. On suppose que pour un entier m , $P(m) = p$. Considérons alors l'expression $P(m + kp)$ où k est un entier naturel.

$$\begin{aligned}
P(m + kp) &= a_n(m + kp)^n + a_{n-1}(m + kp)^{n-1} + \dots + a_1(m + kp) + a_0 \\
&= a_n m^n + a_{n-1} m^{n-1} + \dots + a_1 m + a_0 + pQ(k) \\
&= p + pQ(k) = [1 + Q(k)]p
\end{aligned}$$

où $Q(k)$ est un polynôme en k de degré n .

Cette dernière expression correspond à un nombre composé divisible par p , et ce quelle que soit k .

b. Il n'est donc pas possible de trouver un polynôme à coefficients entiers qui ne prenne que des valeurs premières, puisqu'à partir d'une valeur première, on peut toujours en fabriquer une qui soit composée.

Exercice 73

La raison ne vient pas avec l'âge, elle est dans la tête.

Partie A : Question de cours

1. Énoncer le théorème de Bézout et le théorème de Gauss.

2. Démontrer le théorème de Gauss en utilisant le théorème de Bézout.

Partie B : Il s'agit de résoudre dans $\mathbb{Z}$ le système $(S) \begin{cases} n \equiv 13 [19] \\ n \equiv 6 [12] \end{cases}$.

1. Démontrer qu'il existe un couple $(u; v)$ d'entiers relatifs tel que : $19u + 12v = 1$.

Vérifier, dans ce cas, que le nombre $N = 13 \times 12v + 6 \times 19u$ est une solution du système (S) .

2. a. Soit n_0 une solution de (S) . Vérifier que le système (S) équivaut au système : $\begin{cases} n \equiv n_0 [19] \\ n \equiv n_0 [12] \end{cases}$

b. Démontrer que le système $\begin{cases} n \equiv n_0 [19] \\ n \equiv n_0 [12] \end{cases}$ équivaut à $n \equiv n_0 [12 \times 19]$.

3. a. Trouver un couple $(u; v)$ solution de l'équation $19u + 12v = 1$ et calculer la valeur de N correspondante.

b. Déterminer l'ensemble des solutions de (S) (on pourra utiliser le résultat de la question 2. b.).

4. Un entier naturel n est tel que lorsqu'on le divise par 12 le reste est 6 et lorsqu'on le divise par 19 le reste est 13. On divise n par $228 = 12 \times 19$. Quel est le reste r de cette division ?

Corrigé

Partie A : Voir ton cours d'arithmétique.

Partie B : On sait que $(S) \begin{cases} n \equiv 13 [19] \\ n \equiv 6 [12] \end{cases} \Leftrightarrow \exists k, k' \in \mathbb{Z} \text{ tel que } \begin{cases} n = 13 + 19k \\ n = 6 + 12k' \end{cases}$.

1. Le théorème de Bézout affirme que : 19 et 12 étant premiers entre eux, il existe un couple $(u; v)$ d'entiers relatifs tel que : $19u + 12v = 1$.

Le nombre $N = 13 \times 12v + 6 \times 19u$ est une solution de (S) : en effet, l'entier N peut s'écrire sous la forme $N = 13(1 - 19u) + 6 \times 19u = 13 + 19 \times (-7u)$ car $12v = 1 - 19v$, donc $n \equiv 13 [19]$.

On démontre de même que $n \equiv 6 [12]$.

2. a. Soit n une solution quelconque du système (S) . Donc il existe deux entiers k et k' tels que :

$$\begin{cases} n = 13 + 19k \\ n = 6 + 12k' \end{cases}$$

Si n_0 est une solution de (S) alors il existe deux entiers k_0 et k'_0 tels que : $\begin{cases} n_0 = 13 + 19k_0 \\ n_0 = 6 + 12k'_0 \end{cases}$

D'où par soustraction ligne à ligne, on obtient : $\begin{cases} n - n_0 = 19(k - k_0) \\ n - n_0 = 12(k' - k'_0) \end{cases}$ soit $\begin{cases} n \equiv n_0 [19] \\ n \equiv n_0 [12] \end{cases}$

b. Pour traiter cette question, on établira, de prime abord, le lemme suivant :

$$\text{« Si } \begin{cases} a \text{ divise } c \\ b \text{ divise } c \end{cases} \text{ alors } a \times b \text{ divise } c \text{ »}$$

Preuve :

On a « a divise c » signifie qu'il existe $k_1 \in \mathbb{Z}$ tel que $c = k_1 a$.

De même « b divise c » signifie qu'il existe $k_2 \in \mathbb{Z}$ tel que $c = k_2 b$.

D'autre part, $a \wedge b = 1$ signifie qu'il existe u, v de $\mathbb{Z}$ tels que $au + bv = 1$.

Multiplions cette dernière égalité par c : $acu + bcv = c$. En remplaçant le 1^{er} c par k_2b et le 2^{ème} c par k_1a , on obtient : $a(k_2b)u + b(k_1a)v = ab(k_2u + k_1v) = c$, et comme $k_2u + k_1v$ est un entier alors ab divise c .

On a 19 divise $n - n_0$ de même que 12 ; En vertu du théorème précédent, comme 19 et 12 sont premiers entre eux, alors 19×12 divise $n - n_0$, ce qui équivaut à : $n \equiv n_0 [12 \times 19]$.

3. a. Avec l'algorithme d'Euclide on a $19(-5) + 12(8) = 1$; on peut donc prendre $u = -5$ dans $N = 13 + 19 \times (-7u)$, ce qui donne $N = 678$; de même on prend $v = 8$ et $N = 6 + 12 \times (7v)$, ce qui redonne bien $N = 678$.

b. $N = 678$ est une solution de (S). D'après la question 2.b., les solutions de (S) sont tous les nombres n tels que $n \equiv N [12 \times 19]$ càd $n \equiv 678 [228] \equiv 222 [228]$ car $12 \times 19 = 228$. Donc enfin $S = \{678 + 228k, k \in \mathbb{Z}\}$.

4. Soit n un entier tel que, si on le divise par 12, le reste est 6 et si on le divise par 19, le reste est 13. L'entier n est donc solution de (S). Alors $n \equiv 678 [228] \equiv 222 [228]$. Le reste r de la division de n par $228 = 12 \times 19$ est égal à 222.

Exercice 74

Les yeux ne servent de rien à une cervelle aveugle.

Factorisation d'entiers : la méthode de Fermat

Partie A : Soit N un entier naturel, impair non premier. On suppose que $N = a^2 - b^2$ où a et b sont deux entiers naturels.

1. Montrer que a et b n'ont pas la même parité.
2. Montrer que N peut s'écrire comme produit de deux entiers naturels p et q .
3. Quelle est la parité de p et de q ?

Partie B : On admet que 250 507 n'est pas premier. On se propose de chercher des couples $(a ; b)$ d'entiers naturels vérifiant la relation (E) : $a^2 - 250\,507 = b^2$.

1. Soit X un entier naturel.
 - a. Donner dans un tableau, les restes possibles de X modulo 9 ; puis ceux de X^2 modulo 9.
 - b. Sachant que $a^2 - 250\,507 = b^2$, déterminer les restes possibles modulo 9 de $a^2 - 250\,507$; en déduire les restes possibles modulo 9 de a^2 .
 - c. Montrer que les restes possibles modulo 9 de a sont 1 et 8.
2. Justifier que si le couple $(a ; b)$ vérifie la relation (E), alors $a \geq 501$.

Montrer qu'il n'existe pas de solution du type $(501 ; b)$.

3. On suppose que le couple $(a ; b)$ vérifie la relation (E).
 - a. Démontrer que a est congru à 503 ou à 505 modulo 9.
 - b. Déterminer le plus petit entier naturel k tel que le couple $(505+9k ; b)$ soit solution de (E), puis donner le couple solution correspondant.

Partie C

1. Déduire des parties précédentes une écriture de 250 507 en un produit de deux facteurs.
2. Les deux facteurs sont-ils premiers entre eux ?
3. Cette écriture est-elle unique ?

Corrigé

Partie A

1. Les entiers a et a^2 d'une part, b et b^2 d'autre part, ont même parité, donc si a et b ont même parité, il en est de même de a^2 et b^2 et leur différence $a^2 - b^2$ est paire, ce qui est impossible car N est impair. Donc a et b sont de parité contraire.

2. On a : $N = a^2 - b^2 = (a - b)(a + b)$.

Comme N est un entier naturel non nul (car impair), $a + b$ est un entier naturel non nul, donc $a - b$ et $a + b \in \mathbb{N}$. On peut donc prendre $p = a - b$ et $q = a + b$.

3. Parité de p et q :

Comme a et b sont de parité contraire alors p et q sont impairs selon la question 1.

Partie B

1.a. Restes possibles de X et X^2 modulo 9 :

Les restes possibles de X modulo 9 sont les entiers de 0 à 8. On obtient les restes de X^2 en fonction de ceux de X .

X	0	1	2	3	4	5	6	7	8
X^2	0	1	4	0	7	7	0	4	1

b. Restes possibles de $a^2 - 250\,507$ et a^2 modulo 9 :

On détermine le reste de 250 507 modulo 9. On a : $250\,507 = 27\,834 \times 9 + 1$.

Donc le reste de 250 507 modulo 9 est 1.

D'après la question a. les restes modulo 9 de b^2 sont 0, 1, 4 ou 7. Comme $a^2 = b^2 + 250\,507$ et que le reste de 250 507 est 1, les restes possibles de a^2 modulo 9 sont 1, 2, 5 ou 8.

Mais il résulte aussi de la question a. que les seuls restes possibles de a^2 sont 0, 1 ; 4 ou 7. Finalement, on trouve que le seul reste possible de a^2 modulo 9 est 1.

c. Restes possibles de a modulo 9 : D'après la question a. que a^2 a pour reste 1 modulo 9 si et seulement si : le reste de a modulo 9 est égal à 8.

2. Si (a, b) vérifie (E), on a : $a^2 \geq 250\,507$, soit $a \geq \sqrt{250\,507} > 500$. D'où : $a \geq 501$.

Si $a = 501$, on obtient : $b^2 = 501^2 - 250\,507 = 494$. Or, il n'existe pas d'entier b naturel tel que $b^2 = 494$ (car $22^2 = 484$ et $23^2 = 529$), donc l'équation (E) n'a pas de solution du type $(501, b)$.

3.a. Congruences de a modulo 9

D'après la question 1., l'entier a est congru à 1 ou à 8 modulo 9.

Comme $503 = 9 \times 55 + 8 \equiv 8 [9]$ et $505 = 9 \times 56 + 1 \equiv 1 [9]$, il revient de dire que :

L'entier a est congru à 503 ou à 505 modulo 9.

b. Détermination d'un couple solution :

Le couple $(505 + 9k, b)$ est solution si : $b^2 = (505 + 9k)^2 - 250\,507 = 4\,518 + 9\,090k + 81k^2$

On remarque que $k = 0$ ne convient pas, pour $k = 1$, on obtient :

$$4\,518 + 9\,090 + 81 = 13\,689 = 117^2.$$

Le couple (a, b) correspondant est défini par : $a = 505 + 9 = 514$, $b = 117$.

On a donc trouvé un couple solution : $(514, 117)$.

Partie C

1. Écriture de 250 507 en un produit de deux facteurs

On peut écrire : $250\,507 = 514^2 - 117^2 = (514 + 117)(514 - 117) = 631 \times 397$.

2. On peut vérifier aisément que les entiers 631 et 397 sont premiers et donc ils sont premiers entre eux.

3. Mise à part la décomposition $250\,507 = 1 \times 250\,507$, le nombre 250 507 se décompose de manière unique sous la forme $250\,507 = 631 \times 397$.

Exercice 75

La bougie ne perd rien de sa lumière en la communiquant à une autre bougie.

En factorisant $641 - k^4$ pour $k \in \{1, 2\}$, montrer que le 5^{ème} nombre de Fermat $F_5 = 2^{32} + 1$ n'est pas premier.

Corrigé

On a $641 - 1 = 640 = 5 \times 128 = 5 \times 2^7$, et $641 - 2^4 = 625 = 5^4$.

Ainsi, on peut déduire que :

$$\rightarrow 641 = 5 \times 2^7 + 1 \text{ divise } a = (5 \times 2^7)^4 - 1 = 5^4 \times 2^{28} - 1 \text{ (car } x^4 - 1 = (x - 1)(x + 1)(x^2 + 1))$$

$$\rightarrow 641 = 5^4 + 2^4 \text{ divise } b = 2^{28} \times (5^4 + 2^4) = 5^4 \times 2^{28} + 2^{32}.$$

On en déduit que 641 divise $b - a = (5^4 \times 2^{28} + 2^{32}) - (5^4 \times 2^{28} - 1) = 2^{32} + 1$ c'est-à-dire que 641 divise F_5 et donc F_5 n'est pas premier.

Exercice 76	<i>L'idiot est celui qui cherche des poissons dans les arbres.</i>
--------------------	---

On considère, pour tout $n \in \mathbb{N}^*$, les deux entiers $A = n^2 - 3n + 6$ et $B = n - 2$.

1. Avec $n = 79$, calculer A et B , puis déterminer $\text{PGCD}(A; B)$ en utilisant l'algorithme d'Euclide.
2. Démontrer que, pour tout $n \in \mathbb{N}^*$, on a : $A = B(n - 1) + 4$.
- 3.a. Démontrer que, pour tout a, b et k entiers relatifs, on a : $\text{PGCD}(a; b) = \text{PGCD}(a - kb; b)$.
- b. En déduire l'ensemble des valeurs de n pour lesquelles : $\text{PGCD}(A; B) = 4$.

Corrigé

1. $A = 6010$ et $B = 77$. D'où : $\text{PGCD}(A; B) = \text{PGCD}(77; 4) = \text{PGCD}(4; 1) = \text{PGCD}(1; 0) = 1$

2. $B(n - 1) + 4 = (n - 2)(n - 1) + 4 = n^2 - 3n + 6 = A$

3.a. Si $d|a$ et $d|b$ alors, pour tout $k \in \mathbb{Z}$, $d|a - kb$ et donc : $D(a; b) \subset D(a - kb; b)$

Si $d|a - kb$ et $d|b$ alors pour tout $k \in \mathbb{Z}$, $d|a - kb + kb = a$ et donc : $D(a - kb; b) \subset D(a; b)$

On a prouvé par double inclusion que $D(a; b) = D(a - kb; b)$ donc que :

$$\text{PGCD}(a; b) = \text{PGCD}(a - kb; b).$$

b. Valeurs de n pour que $\text{PGCD}(A; B) = 4$

$$\text{PGCD}(A; B) = 4 \Leftrightarrow \text{PGCD}(A - B(n - 1); B) = 4 \Leftrightarrow \text{PGCD}(4; B) = 4$$

$$\Leftrightarrow 4|B \Leftrightarrow n - 2 = 4k \text{ avec } k \text{ entier relatif}$$

$$\Leftrightarrow n = 4k + 2 \text{ avec } k \text{ entier relatif}$$

Exercice 77	<i>La patience ne connaît pas le temps.</i>
--------------------	--

1. Montrer que pour tout entier $n : (n + 2)(5n^2 - 10n + 19) - 38 = 5n^3 - n$.

2.a. En déduire que : $\text{PGCD}(5n^3 - n, n + 2) = \text{PGCD}(n + 2, 38)$.

b. Lorsque $d = \text{PGCD}(5n^3 - n, n + 2)$, quelles sont les valeurs possibles de d ?

3. Résoudre $\text{PGCD}(5n^3 - n, n + 2) = 19$.

Corrigé

1. Un simple développement permet d'établir que : $(n + 2)(5n^2 - 10n + 19) - 38 = 5n^3 - n$.

2.a. Soit a, b, c et d des entiers. Pour démontrer que $\text{PGCD}(a, b) = \text{PGCD}(c, d)$, il suffit de montrer que l'ensemble des diviseurs communs à a et b est le même que l'ensemble des diviseurs communs à c et d .

L'écriture $(n + 2)(5n^2 - 10n + 19) - 38 = 5n^3 - n$ nous permet de dire que tout diviseur commun à $5n^3 - n$ et $n + 2$ est diviseur commun à $n + 2$ et 38. Réciproquement, tout diviseur commun à $n + 2$ et 38 est diviseur commun à $5n^3 - n$ et $n + 2$. Il vient donc :

$$\text{PGCD}(5n^3 - n, n + 2) = \text{PGCD}(n + 2, 38).$$

b. Comme d doit diviser 38, les valeurs possibles de d sont 1, 2, 19 et 38.

3. D'après la question précédente, résoudre $\text{PGCD}(5n^3 - n, n + 2) = 19$ revient à résoudre l'équation $\text{PGCD}(n + 2, 38) = 19$. Cela veut dire qu'il existe des entiers p et q tels que $n + 2 = 19p$ et $38 = 19q$ avec p et q premiers entre eux. Il est clair que q est pair. Le fait que p et q sont premiers entre eux impose que p est impair. Donc n est de la forme : $n = 19(2k + 1) - 2$.

Exercice 78	<i>Quand on cède à la peur du mal, on ressent déjà le mal de la peur.</i>
--------------------	--

Une formule pour calculer le PGCD

Soient a et b deux entiers positifs, montrer que :

$$a \wedge b = a + b - ab + 2 \sum_{k=1}^{b-1} E\left(k \frac{a}{b}\right) \text{ où } E(x) \text{ est la partie entière de } x.$$

Cette formule a été trouvée par Marcelo Pólezzi en 1997.

Corrigé

Posons $d = a \wedge b$.

On sait qu'il existe deux naturels a' et b' premiers entre eux tels que $a = da'$ et $b = db'$.

Lorsque k décrit $\{0, 1, \dots, b-1\}$, $k \frac{a}{b} = k \frac{a'}{b'}$ est un entier si et seulement si b' divise k . Ceci se produit exactement $E\left(\frac{b-1}{b'}\right) = E\left(d - \frac{1}{b'}\right) = d - 1$ fois.

Or, on a :

$$E\left(k \frac{a}{b}\right) + E\left(a - k \frac{a}{b}\right) = \begin{cases} a - 1 & \text{si } k \frac{a}{b} \notin \mathbb{N} \\ a & \text{si } k \frac{a}{b} \in \mathbb{N} \end{cases}$$

Ainsi :

$$\sum_{k=1}^{b-1} \left[E\left(k \frac{a}{b}\right) + E\left(a - k \frac{a}{b}\right) \right] = (a-1)(b-1) + (d-1) = ab - a - b + d$$

Pour conclure, on a :

$$\begin{aligned} 2 \sum_{k=1}^{b-1} \left(E\left(k \frac{a}{b}\right) \right) &= \sum_{k=1}^{b-1} \left(E\left(k \frac{a}{b}\right) \right) + \sum_{k=1}^{b-1} \left(E\left((b-k) \frac{a}{b}\right) \right) = \sum_{k=1}^{b-1} \left(E\left(k \frac{a}{b}\right) \right) + \sum_{k=1}^{b-1} \left(E\left(a - k \frac{a}{b}\right) \right) \\ &= ab - a - b + d \end{aligned}$$

D'où le résultat escompté.

Exercice 79

Un proverbe est l'esprit d'un seul et la sagesse de tous.

Triplets pythagoriciens

Dans cet exercice, on s'intéresse aux triplets d'entiers naturels non nuls (x, y, z) tels que :

$$x^2 + y^2 = z^2$$

Ces triplets seront nommés « triplets pythagoriciens » en référence aux triangles rectangles dont ils mesurent les côtés, et notés en abrégé « TP ». Ainsi $(3, 4, 5)$ est un TP car $3^2 + 4^2 = 5^2$.

Partie A : généralités

1. Démontrer que, si (x, y, z) est un TP, et p un naturel non nul, alors le triplet (px, py, pz) est lui aussi un TP.

2. Démontrer que, si (x, y, z) est un TP, alors les naturels x, y et z ne peuvent pas être tous les trois impairs.

3. Pour cette question, on admet que tout entier naturel non nul n peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair :

$$n = 2^\alpha \times k \text{ où } \alpha \text{ est un entier naturel (éventuellement nul) et } k \text{ un entier naturel impair.}$$

L'écriture $n = 2^\alpha \times k$ est nommée décomposition de n .

Voici par exemple les décompositions des entiers 9 et 120 : $9 = 2^0 \times 9$, $120 = 2^3 \times 15$.

a. Donner la décomposition de l'entier 192.

b. Soient x et z deux entiers naturels non nuls, dont les décompositions sont $x = 2^\alpha \times k$ et $z = 2^\beta \times m$. Écrire la décomposition des entiers naturels $2x^2$ et z^2 .

c. En examinant l'exposant de 2 dans la décomposition de $2x^2$ et dans celle de z^2 , montrer qu'il n'existe pas de couple d'entiers naturels non nuls (x, z) tels que $2x^2 = z^2$.

On admet que la question A - 3. permet d'établir que les trois entiers naturels x, y et z sont deux à deux distincts. Comme de plus les entiers naturels x, y jouent un rôle symétrique, dans la suite, pour tout TP (x, y, z) , les trois entiers naturels x, y et z seront rangés dans l'ordre suivant : $x < y < z$.

Partie B : recherche de triplets pythagoriciens contenant l'entier 2015

1. Décomposer en produit de facteurs premiers l'entier 2 015 puis, en utilisant le TP donné dans le préambule, déterminer un TP de la forme $(x, y, 2015)$.

2. On admet que, pour tout entier naturel n , on a : $(2n+1)^2 + (2n^2+2n)^2 = (2n^2+2n+1)^2$.

Déterminer un TP de la forme $(2015, y, z)$.

3. a. En remarquant que $403^2 = 169 \times 961$, déterminer un couple d'entiers naturels non nuls (x, z) tels que

$$z^2 - x^2 = 403^2, \text{ avec } x < 403.$$

b. En déduire un TP de la forme $(x, 2015, z)$.

Corrigé

Partie A : généralités

1. Soit $(x; y; z)$ un TP et soit p un entier naturel non nul. On a donc $x^2 + y^2 = z^2$. Alors :

$(px)^2 + (py)^2 = p^2x^2 + p^2y^2 = p^2(x^2 + y^2) = p^2z^2 = (pz)^2$. Donc $(px; py; pz)$ est aussi un TP.

2. On suppose que $(x; y; z)$ est un TP donc $x^2 + y^2 = z^2$. Supposons les trois entiers impairs.

Alors : $x \equiv 1 [2], y \equiv 1 [2]$ et $z \equiv 1 [2]$.

On a : $x^2 \equiv 1 [2], y^2 \equiv 1 [2]$ et $z^2 \equiv 1 [2]$, d'où $x^2 + y^2 \equiv 0 [2]$ donc on n'aurait pas $x^2 + y^2 = z^2$.

Les trois entiers ne peuvent pas être tous impairs.

3. Pour cette question, on admet que tout entier naturel non nul n peut s'écrire d'une façon unique sous la forme du produit d'une puissance de 2 par un entier impair : $n = 2^\alpha \times k$ où α est un entier naturel (éventuellement nul) et k un entier naturel impair.

a. $192 = 2^6 \times 3$.

b. Soient x et z deux entiers naturels non nuls, dont les décompositions sont $x = 2^\alpha \times k$ et $z = 2^\beta \times m$.

On a : $2x^2 = 2 \times (2^\alpha \times k)^2 = 2 \times 2^{2\alpha} \times k^2 = 2^{2\alpha+1} \times k^2$ et $z^2 = (2^\beta \times m)^2 = 2^{2\beta} \times m^2$.

c. Si $2x^2 = z^2$, alors $2^{2\alpha+1} \times k^2 = 2^{2\beta} \times m^2$ donc $2\alpha + 1 = 2\beta$ (unicité de la décomposition). C'est impossible puisque $2\alpha + 1$ est impair et 2β est pair.

Partie B : recherche de triplets pythagoriciens contenant l'entier 2015

1. $2015 = 5 \times 13 \times 31$. On connaît le TP $(3; 4; 5)$ donc $(13 \times 31 \times 3; 13 \times 31 \times 4; 13 \times 31 \times 5)$ est aussi un TP, donc $(1209; 1612; 2015)$ est aussi un TP.

2. On admet que, pour tout entier naturel n , on a : $(2n + 1)^2 + (2n^2 + 2n)^2 = (2n^2 + 2n + 1)^2$.

Or $2015 = 2 \times 1007 + 1$, donc, d'après la remarque faite ci-dessus, le triplet :

$(2015; 2 \times 1007^2 + 2 \times 1007; 2 \times 1072 + 2 \times 107 + 1)$ c'est-à-dire que le triplet $(2015; 2030112; 2030113)$ est un TP.

3. a. On cherche x et z entiers tels que $z^2 - x^2 = 403^2$, c'est-à-dire : $(z - x)(z + x) = 169 \times 961$.

Réolvons le système $\begin{cases} z - x = 169 \\ z + x = 961 \end{cases}$. En additionnant et en soustrayant, on trouve $z = 565$ et $x = 396$.

b. Le triplet $(396; 403; 565)$ est un TP donc $(5 \times 396; 5 \times 403; 5 \times 565)$ est également un TP. Par conséquent $(1980; 2015; 2825)$ est un TP.

Exercice 80

Pour la bouche, on n'a pas encore fabriqué de portes à serrure.

Les nombres complexes au service de l'arithmétique

On dit qu'un entier naturel A est somme de deux carrés, s'il existe deux entiers naturels x et y tels que :

$$A = x^2 + y^2$$

On se propose de démontrer que, si A est somme de deux carrés alors A^n est aussi somme de deux carrés, pour tout entier $n \geq 1$. Soit x et y deux entiers et z le nombre complexe : $z = x + iy$.

1. Montrer par récurrence que $z^n = x_n + iy_n$, avec x_n et y_n entiers.

2. Prouver alors que si $A = x^2 + y^2$ alors $A^n = x_n^2 + y_n^2$.

3. Conclure.

4. Sachant que $25 = 3^2 + 4^2$ et que $390\,625 = 25^4$, écrire $390\,625$ sous la forme de la somme de deux carrés.

Corrigé

1. La propriété est vraie pour $n = 1$ ($x_1 = x$ et $y_1 = y$). Soit $n \geq 1$. On suppose que $z^n = x_n + iy_n$ avec x_n et y_n entiers et n entier donné. On a : $z^{n+1} = z^n \times z = (x_n + iy_n)(x_1 + iy_1) = (x_nx_1 - y_ny_1) + i(x_ny_1 + x_1y_n)$

En posant $x_{n+1} = x_nx_1 - y_ny_1$ et $y_{n+1} = x_ny_1 + x_1y_n$, on peut écrire : $z^{n+1} = x_{n+1} + iy_{n+1}$.

Ce qui démontre la propriété car x_{n+1} et y_{n+1} entiers.

2. On a : $A = x^2 + y^2 = (x + iy)(x - iy) = z\bar{z}$ avec x et y entiers. Donc :

$$A^n = z^n \times \overline{z^n} = (x_n + iy_n)(x_n - iy_n) = x_n^2 + y_n^2$$

3. D'après la question précédente que si A est somme de deux carrés alors A^n est aussi somme de deux carrés.

4. On a : $25 = 3^2 + 4^2 = (3 + 4i)(3 - 4i)$ et donc :

$$25^2 = (3 + 4i)^2(3 - 4i)^2 = (-7 + 24i)(-7 - 24i) \text{ et}$$

$$(25^2)^2 = (-7 + 24i)^2(-7 - 24i)^2 = (-527 - 336i)(-527 + 336i) = 527^2 + 336^2. \text{ Donc enfin :}$$

$$390\,625 = 527^2 + 336^2.$$

Exercice 81

Quand l'eau baisse, les fourmis mangent les poissons ; quand l'eau monte, les poissons mangent les fourmis.

Lorsque les nombres complexes s'invitent en arithmétique

Un entier n est dit somme de deux carrés s'il existe deux entiers a et b tels que $n = a^2 + b^2$. Montrer que si n et p sont sommes de deux carrés alors leur produit $n \times p$ l'est aussi. Par exemple, on a : $5 = 2^2 + 1^2$ et $401 = 20^2 + 1^2$, quelle est la décomposition en somme de deux carrés de 2005 ?

Corrigé

L'expression $n = a^2 + b^2$ peut aussi s'écrire $n = |a + ib|^2$. Ainsi si $p = c^2 + d^2$, on a :

$$n \times p = |a + ib|^2 \times |c + id|^2 = |(a + ib) \times (c + id)|^2 = |(ac - bd) + i(ad + bc)|^2 \\ = (ac - bd)^2 + (ad + bc)^2$$

Donc $n \times p$ est bien la somme de deux carrés.

On a également : $n \times p = |b + ia|^2 \times |c + id|^2 = (bc - ad)^2 + (bd + ac)^2$ car $|b + ia| = |a + ib|$.

Ainsi, comme $5 = 2^2 + 1^2$ et $401 = 20^2 + 1^2$ et $2005 = 5 \times 401$ on peut écrire :

$$2005 = (2 \times 20 - 1 \times 1)^2 + (2 \times 1 + 20 \times 1)^2 = 39^2 + 22^2$$

$$2005 = (2 \times 1 - 1 \times 20)^2 + (2 \times 20 + 1 \times 1)^2 = 18^2 + 41^2.$$

Exercice 82

Mieux vaut une vérité qui fait pleurer qu'un mensonge qui fait rire.

On considère la suite (u_n) d'entiers naturels : $u_0 = 14, u_{n+1} = 5u_n - 6$ pour tout naturel n .

1. Calculer u_1, u_2, u_3 et u_4 .

Quelle conjecture peut-on émettre concernant les deux derniers chiffres du nombre u_n ?

2. Montrer que, pour tout entier naturel n , $u_{n+2} \equiv u_n \pmod{4}$.

En déduire que pour tout entier naturel k , $u_{2k} \equiv 2 \pmod{4}$ et $u_{2k+1} \equiv 0 \pmod{4}$.

3. a. Montrer par récurrence que, pour tout entier naturel n , $2u_n = 5^{n+2} + 3$.

b. En déduire que, pour tout entier naturel n , $2u_n \equiv 28 \pmod{100}$.

4. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n .

5. Montrer que le PGCD de deux termes consécutifs de la suite (u_n) est constant. Préciser sa valeur.

Corrigé

1. On calcule $u_1 = 64, u_2 = 314, u_3 = 1\,564, u_4 = 7\,814$.

On peut conjecturer que les termes u_{2k} se terminent par 14 et les termes u_{2k+1} se terminent par 64.

2. On a : $u_{n+2} = 5u_{n+1} - 6 = 5(5u_n - 6) - 6 = 25u_n + 36$. Or, on remarque que :

$$24u_n + 36 \equiv 0 \pmod{4}, \text{ d'où :}$$

$$u_{n+2} \equiv (u_n + 24u_n + 36) \pmod{4} \equiv (u_n + 0) \equiv u_n \pmod{4}$$

On démontre par récurrence que pour tout entier k : $u_{2k} \equiv 2 \pmod{4}$ et $u_{2k+1} \equiv 0 \pmod{4}$ car pour tout entier k , on a : $u_{2k} \equiv u_0 \pmod{4}$ et $u_{2k+1} \equiv u_1 \pmod{4}$.

3. a. Établissons par récurrence l'égalité $2u_n = 5^{n+2} + 3$.

Pour $n = 0$: $2u_0 = 28 = 5^2 + 3$: l'égalité est vraie à ce rang.

Supposons qu'il existe un entier n tel que l'on ait $2u_n = 5^{n+2} + 3$. Alors, on a :

$$2u_{n+1} = 2(5u_n - 6) = 5 \times 2u_n - 12 = 5(5^{n+2} + 3) - 12 = 5^{n+3} + 15 - 12 = 5^{(n+1)+2} + 3$$

La relation est donc vraie au rang $n + 1$.

b. On sait déjà que $2u_n = 5^{n+2} + 3$, or $5^n \equiv 1 \pmod{4}$ et par suite, en multipliant et même le modulo par 25, on obtient $5^{n+2} \equiv 25 \pmod{100}$. Donc $2u_n \equiv 25 + 3 \pmod{100}$ i.e $2u_n \equiv 28 \pmod{100}$.

4. La relation $2u_n \equiv 28 \pmod{100}$ s'écrit $2u_n \equiv 28 + 100h$ avec $h \in \mathbb{N}$, soit $u_n \equiv 14 + 50h$.

Or on sait que :

Si $n = 2k$, $u_n \equiv 14 + 50h = 2 + 4m$ ($m \in \mathbb{N}$), d'où : $6 + 25h = 2m$ et donc h est pair : $h = 2p$ et par suite : $u_{2k} = 14 + 100p$, donc les deux derniers chiffres de u_{2k} sont 14.

On démontre de manière analogue que les deux derniers chiffres de u_{2k+1} sont 64.

5. On voit que le $\text{PGCD}(u_0, u_1) = \text{PGCD}(14, 64) = 2$; il faut donc montrer : $\text{PGCD}(u_n, u_{n+1}) = 2$.

On pose pour tout n , $\text{PGCD}(u_n, u_{n+1}) = d$. Comme on a $5u_n - u_{n+1} = 6$, la relation de Bézout montre que d est un diviseur de 6. Donc $d \in \{1, 2, 3, 6\}$.

→ Si $d = 3$ alors 3 divise u_n et donc 3 divise $2u_n = 5^{n+2} + 3$.

Ce qui est impossible car 3 ne divise pas 5^{n+2} .

→ Si $d = 6$ alors 6 divise u_n et donc 6 divise $2u_n$, ce qui est impossible car 3 ne divise pas $2u_n$.

Comme pour tout n , u_n est pair alors $\text{PGCD}(u_n, u_{n+1}) = 2$.

Exercice 83

Il n'est pas possible d'être mathématicien sans avoir l'âme d'un poète.

Soit la suite de terme général $u_n = 2^{3^n} + 3^{3^n}$ pour $n \in \mathbb{N}^*$. Le but de l'exercice est de démontrer, par récurrence, que u_n possède au moins $n + 1$ diviseurs premiers distincts.

Soit la propriété $\wp(n)$: « $\forall n \geq 1$, u_n possède $n + 1$ diviseurs premiers».

1. Initialisation :

Vérifier que $\wp(1)$ est vraie.

2. Hérédité :

On suppose que la propriété $\wp(n)$ est vraie pour un certain rang $n \in \mathbb{N}^*$. Posons $X = 2^{3^n}$ et $Y = 3^{3^n}$.

a. Montrer que $u_{n+1} = (X^2 - XY + Y^2)u_n$. En déduire que u_{n+1} admet au moins $n + 1$ diviseurs premiers distincts.

b. Montrer que $X^2 - XY + Y^2$ admet au moins un diviseur premier p .

c. Montrer, à l'aide d'un raisonnement par l'absurde, que p ne divise pas u_n .

3. Conclure.

Corrigé

1. On a : $u_1 = 2^3 + 3^3 = 35$, qui possède 2 diviseurs premiers distincts à savoir 5 et 7, donc on a $\wp(1)$.

2. Supposons que $\wp(n)$ soit vraie pour un certain rang $n \in \mathbb{N}^*$.

a. On a : $u_{n+1} = 2^{3^{n+1}} + 3^{3^{n+1}} = (2^{3^n})^3 + (3^{3^n})^3 = X^3 + Y^3$.

Or, on sait que $X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2)$ et $X + Y = u_n$, d'où : $u_{n+1} = (X^2 - XY + Y^2)u_n$.

Comme $X^2 - XY + Y^2$ est un entier alors u_n divise u_{n+1} et par suite tout diviseur premier de u_n est également diviseur premier de u_{n+1} . Donc en vertu de l'hypothèse de récurrence, on peut déduire que u_{n+1} admet au moins $n + 1$ diviseurs premiers distincts.

b. Il suffit de s'assurer que $X^2 - XY + Y^2 \geq 2$.

On a : $X^2 - XY + Y^2 = (X - Y)^2 + XY \geq 2$ car $XY = 2^{3^n} \times 3^{3^n} \geq 2$ pour $n \geq 1$.

Donc $X^2 - XY + Y^2$ étant un entier supérieur à 2, il admet au moins un diviseur premier p .

c. On raisonne par l'absurde en supposant que p divise $u_n = X + Y$. On a : p divise $X + Y$ et p divise $X^2 - XY + Y^2$ implique que p divise toute combinaison linéaire de $X + Y$ et $X^2 - XY + Y^2$.

On remarque que $X^2 - XY + Y^2 = (X + Y)^2 - 3XY$ c'est-à-dire :

$$(X^2 - XY + Y^2) - (X + Y)^2 = -3XY$$

Donc p divise $3XY = 2^{3^n} \times 3^{3^n+1}$ et donc $p = 2$ ou $p = 3$ en vertu de l'unicité de la décomposition d'un entier supérieur à 2 en produit de facteurs premiers. Ce qui est impossible car si 2 ou si 3 diviserait $u_n = 2^{3^n} + 3^{3^n}$ alors 2 divise 3^{3^n} ou 3 divise 2^{3^n} ; ce qui est vachement faux. Donc p ne divise pas u_n et par conséquent u_{n+1} possède au moins $(n + 1) + 1 = n + 2$ diviseurs premiers distincts.

3. La propriété $\wp(n)$ est vraie pour $n = 1$ et héréditaire à partir de 1, donc pour $n \geq 1$, $\wp(n)$ est vraie.

Ainsi le nombre $A = 2^{3^{2016}} + 3^{3^{2016}}$ possède au moins 2017 diviseurs premiers distincts.

Exercice 84

Un homme sans ami, c'est la main gauche sans la droite.

1. Montrer que pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x - 1)(1 + x + x^2 + \cdots + x^{k-1}) = x^k - 1.$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. a. Soit $n \in \mathbb{N}^*$ et d un diviseur positif de n : $n = dk$. Montrer que $a^d - 1$ est un diviseur de $a^n - 1$.

- b. Dédurre de la question précédente que $2^{2004} - 1$ est divisible par 7, par 63 puis par 9. $2^{60} - 1$
3. Soient m et n deux entiers naturels non nuls et d leur PGCD.
- a. On définit m' et n' par $m = dm'$ et $n = dn'$. En appliquant le théorème de Bézout à m' et n' , montrer qu'il existe des entiers relatifs u et v tels que : $mu - nv = d$.
- b. On suppose u et v strictement positifs. Montrer que : $(a^{mu} - 1) - (a^{nv} - 1)a^d = a^d - 1$.
Montrer ensuite que $a^d - 1$ est le PGCD de $a^{mu} - 1$ et de $a^{nv} - 1$.
- c. Calculer, en utilisant le résultat précédent, le PGCD de $2^{63} - 1$ et de $2^{60} - 1$.

Corrigé

1. Pour montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x - 1)(1 + x + x^2 + \dots + x^{k-1}) = x^k - 1,$$

on développe le terme de gauche :

$$(x - 1)(1 + x + \dots + x^{k-1}) = x + x^2 + \dots + x^{k-1} + x^k - 1 - x - x^2 - \dots - x^{k-1} = x^k - 1.$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. a. Soit n un entier naturel non nul et d un diviseur positif de n : $n = dk$.

D'après 1, on peut écrire :

$$a^n - 1 = a^{dk} - 1 = (a^d)^k - 1 = (a^d - 1)(1 + a^d + (a^d)^2 + \dots + (a^d)^{k-1}),$$

donc $a^d - 1$ est un diviseur de $a^n - 1$.

b. On sait que $2004 = 3 \times 668 = 6 \times 334$. Donc $2^{2004} - 1$ est divisible par $2^3 - 1 = 7$, et par $2^6 - 1 = 63$. Donc $2^{2004} - 1 = 63k$ avec $k \in \mathbb{Z}$, d'où $2^{2004} - 1 = 7 \times 9k$, ce qui prouve que $2^{2004} - 1$ est divisible par 9.

3. Soient m et n deux entiers naturels non nuls et d leur PGCD.

a. On définit m' et n' par $m = dm'$ et $n = dn'$. On sait que dans ce cas, les entiers m' et n' sont premiers entre eux, donc d'après le théorème de Bézout, il existe des entiers u et v tels que : $m'u - n'v = 1$.

Soit en multipliant par d , on trouve $mu - nv = d$.

b. On suppose u et v strictement positifs. On peut écrire $mu = nv + d$. On a :

$$\begin{aligned} (a^{mu} - 1) - (a^{nv} - 1)a^d &= a^{mu} - 1 - a^{nv} \times a^d + a^d \\ &= a^{mu} - 1 - a^{nv+d} + a^d = a^{mu} - 1 - a^{mu} + a^d = a^d - 1 \end{aligned}$$

Cette relation est de la forme $AU + BV = a^d - 1$.

D'après la question 2, $a^d - 1$ divise $a^{mu} - 1$ et $a^{nv} - 1$; de plus, la relation précédente prouve que le PGCD de $a^{mu} - 1$ et de $a^{nv} - 1$ divise $a^d - 1$; donc $a^d - 1$ est le PGCD de $a^{mu} - 1$ et de $a^{nv} - 1$.

c. On sait que $\text{PGCD}(60; 63) = 3$, donc en utilisant le résultat précédent, on conclut que le PGCD de $2^{63} - 1$ et de $2^{60} - 1$ est $2^3 - 1 = 7$.

Exercice 85

Si tu dors et que tu rêves que tu dors, il faut que tu te réveilles deux fois pour te lever.

1. On considère l'équation (1) d'inconnue $(n; m)$ élément de $\mathbb{Z}^2$: $11n - 24m = 1$.

a. Justifier, à l'aide de l'énoncé d'un théorème, que cette équation admet au moins une solution.

b. En utilisant l'algorithme d'Euclide, déterminer une solution particulière de l'équation (1).

c. Déterminer l'ensemble des solutions de l'équation (1).

2. Recherche du PGCD de $10^{11} - 1$ et $10^{24} - 1$.

a. Justifier que 9 divise $10^{11} - 1$ et $10^{24} - 1$.

b. (n, m) désignant un couple quelconque d'entiers naturels solutions de (1), montrer que l'on peut alors écrire :

$$(10^{11n} - 1) - 10(10^{24m} - 1) = 9.$$

c. Montrer que $10^{11} - 1$ divise $10^{11n} - 1$.

(on rappelle l'égalité : $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a^1 + 1)$, valable pour tout naturel n non nul).

Dédurre de la question précédente l'existence de deux entiers N et M tels que :

$$(10^{11} - 1)N - (10^{24} - 1)M = 9.$$

d. Montrer que tout diviseur commun à $10^{24} - 1$ et $10^{11} - 1$ divise 9.

e. Dédurre des questions précédentes le P.G.C.D. de $10^{24} - 1$ et $10^{11} - 1$.

3. a. Justifier que $10^{12} \equiv 1 [13]$.

b. En déduire que $10^{24} - 1$ est divisible par 13.

- c. De la même manière, montrer que $10^{24} - 1$ est divisible par 7.
d. En déduire que $10^{24} - 1$ est divisible par 273.

Corrigé

1. On considère l'équation (1) d'inconnue (n, m) élément de $\mathbb{Z}^2$: $11n - 24m = 1$.
a. Le théorème de Bézout affirme que si 11 et 24 sont premiers entre eux, alors l'équation : $11n - 24m = 1$ admet des solutions entières. Or 11 est premier et ne divise pas 24, donc 11 et 24 sont premiers entre eux.
b. On utilise l'algorithme d'Euclide : $24 = 11 \times 2 + 2$, $11 = 2 \times 5 + 1$. D'où :
 $1 = 11 - 2 \times 5 = 11 - (24 - 11 \times 2) \times 5 = 11 \times 11 - 5 \times 24$.
Donc une solution de (1) est le couple $(11; 5)$.
c. Par différence, $11(n - 11) - 24(m - 5) = 0$, soit $11(n - 11) = 24(m - 5)$. D'après le théorème de Gauss, comme 11 et 24 sont premiers entre eux, alors 24 divise $n - 11$, soit $n - 11 = 24k$ avec $k \in \mathbb{Z}$, ou encore $n = 24k + 11$. En remplaçant $n - 11$ dans $11(n - 11) = 24(m - 5)$, on trouve $m - 5 = 11k$, soit $m = 11k + 5$. L'ensemble des solutions de l'équation (1) est : $\{(24k + 11; 11k + 5)/k \in \mathbb{Z}\}$.
2. Recherche du PGCD de $10^{11} - 1$ et $10^{24} - 1$.
a. On a $10 \equiv 1 [9]$, donc pour tout naturel n , $10^n \equiv 1 [9]$, donc $10^{11} - 1 \equiv 0 [9]$, et $10^{24} \equiv 1 [9]$, soit $10^{24} - 1 \equiv 0 [9]$. Donc 9 divise $10^{11} - 1$ et $10^{24} - 1$.
b. $(n; m)$ désignant un couple d'entiers naturels solutions de (1), alors $10^{11n} = 10^{1+24m}$. Ainsi, on a :
 $(10^{11n} - 1) - 10(10^{24m} - 1) = 10^{11n} - 1 - 10^{24m+1} + 10 = 10^{11} - 1 - 10^{11n} + 10 = 9$.
c. D'après l'égalité $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a^1 + 1)$, on peut écrire :
 $10^{11} - 1 = (10^{11} - 1)(10^{11(n-1)} + 10^{11(n-2)} + \dots + 1)$, donc $10^{11} - 1$ divise $10^{11n} - 1$. De la même manière, on prouve que : $10^{24} - 1$ divise $10^{24m} - 1$. Soit $10^{11n} - 1 = N(10^{11} - 1)$ et $10^{24m} - 1 = M'(10^{24} - 1)$ alors de la relation : $(10^{11n} - 1) - 10(10^{24m} - 1) = 9$, on déduit :
 $N(10^{11} - 1) - 10M'(10^{24} - 1) = N(10^{11} - 1) - M(10^{24} - 1) = 9$, avec $10M' = M$.
Donc il existe deux entiers N et M tels que : $(10^{11} - 1)N - (10^{24} - 1)M = 9$.
d. Par le théorème de Bézout, l'équation $(10^{11} - 1)N - (10^{24} - 1)M = 9$ a des solutions si et seulement si le PGCD de $10^{24} - 1$ et $10^{11} - 1$ divise 9. Donc tout diviseur commun à $10^{24} - 1$ et $10^{11} - 1$ divise 9.
e. On a vu que le PGCD de $10^{24} - 1$ et $10^{11} - 1$ divise 9 et que $10^{24} - 1$ et $10^{11} - 1$ sont divisibles par le nombre 9, donc le P.G.C.D. de $10^{24} - 1$ et $10^{11} - 1$ est 9.
3. a) Par le théorème de Fermat, 13 est un nombre premier et 10 est premier avec 13, donc $10^{12} \equiv 1 [13]$.
b) On en déduit que $10^{24} = (10^{12})^2 \equiv 1^2 \equiv 1 [13]$. Donc $10^{24} - 1$ est divisible par 13.
c) Par le théorème de Fermat, 7 est un nombre premier et 10 est premier avec 7, donc $10^6 \equiv 1 [7]$. On en déduit que $10^{24} = (10^6)^4 \equiv 1^4 \equiv 1 [7]$. Donc $10^{24} - 1$ est divisible par 7.
d) De plus, $10 \equiv 1 [3]$, donc $10^{24} \equiv 1^{24} \equiv 1 [3]$. Donc $10^{24} - 1$ est divisible par 3. Ainsi $10^{24} - 1$ est divisible par 3, 7 et 13 qui sont premiers entre eux, donc $10^{24} - 1$ est divisible par $3 \times 7 \times 13 = 273$.

Exercice 86

Le mensonge donne des fleurs mais pas de fruits.

1. On considère x et y des entiers relatifs et l'équation (E) : $91x + 10y = 1$.
a. Énoncer un théorème permettant de justifier l'existence d'une solution à (E).
b. Déterminer une solution particulière de (E) et en déduire une solution particulière de l'équation (E') :

$$91x + 10y = 412.$$

c. Résoudre (E'). $A_3x + A_2y = 3296$
2. Montrer que les nombres $A_n = 3^{2n} - 1$, où n est un naturel non nul, sont divisibles par 8.
3. On considère l'équation (E'') : $A_3x + A_2y = 3296$.
a. Déterminer les couples d'entiers relatifs (x, y) solutions de l'équation (E'').
b. Montrer que (E'') admet pour solution un couple unique d'entiers naturels. Le déterminer.

Corrigé

1. a. 91 et 10 étant premiers entre eux, l'équation (E) admet des solutions (théorème de Bézout.)
b. Le couple $(1; -9)$ est une solution particulière de (E) et donc :

$(412 = 412 \times 1; -3708 = 412 \times (-9))$ est une solution particulière de l'équation (E') .

c. Soit $(x; y)$ une solution de (E') . On a : $\begin{cases} 91x + 10y = 412 \\ 91 \times 412 + 10 \times (-3708) = 412 \end{cases}$ et donc par différence, on obtient : $91(x - 412) = -10(y + 3708)$ (1)

Comme 91 divise $10(y + 3708)$ et que 91 et 10 sont premiers entre eux, Gauss nous permet de conclure que l'entier 91 divise $y + 3708$. Donc, il existe un entier relatif k tel que $y + 3708 = 91k$, soit donc :

$$y = 91k - 3708.$$

En remplaçant $y + 3708$ par $91k$ dans (1), on obtient : $x = 412 - 10k$.

Donc l'ensemble des solutions de (E') est : $S_{(E')} = \{(412 - 10k; 91k - 3708)/k \in \mathbb{Z}\}$.

2. On a : $3^2 = 9 \equiv 1 [8]$ et donc $3^{2n} = (3^2)^n \equiv 1^n [8]$. Donc $3^{2n} - 1 \equiv 0 [8]$ càd 8 divise $3^{2n} - 1$.

3. a. On a : $A_3 = 728$ et $A_2 = 80$ et donc l'équation (E'') s'écrit : $728x + 80y = 3296$.

On remarque que les coefficients 728, 80 et 3296 sont tous divisibles par 8 : $\begin{cases} 728 = 8 \times 91 \\ 80 = 8 \times 10 \\ 3296 = 8 \times 412 \end{cases}$

Donc l'équation (E'') est équivalente à $91x + 10y = 412$. D'où l'ensemble des solutions de (E'') est le même que celui de l'équation (E') .

b. Il faut que les solutions soient positives : il s'agit de déterminer un entier relatif k tel que :

$$\begin{cases} x = 412 - 10k \geq 0 \\ y = 91k - 3708 \geq 0 \end{cases}$$

On a : $\begin{cases} x = 412 - 10k \geq 0 \\ y = 91k - 3708 \geq 0 \end{cases} \Leftrightarrow \begin{cases} k \leq 41,2 \\ k \geq 40,7 \end{cases}$ soit $k = 41$.

Pour $k = 41$, on obtient $x = 412 - 10 \times 41 = 2$ et $y = 91 \times 41 - 3708 = 23$.

Donc l'unique couple solution est $(2; 23)$.

Exercice 87

Il n'y a pas de problème. Il n'y a que des professeurs.

Soit a un entier naturel non nul et (u_n) la suite définie par :

$$\begin{cases} u_0 = 2 \text{ et } u_1 = 2a + 1 \\ u_{n+2} = (2a + 1)u_{n+1} - a(a + 1)u_n, \forall n \in \mathbb{N} \end{cases}$$

1.a. Soit α, β et γ trois entiers.

Montrer que ① $\begin{cases} \alpha \wedge \beta = 1 \\ \alpha \wedge \gamma = 1 \end{cases} \Rightarrow \alpha \wedge (\beta\gamma) = 1$ (où $x \wedge y = \text{PGCD}(x, y)$).

b. Soit A, B, X et Y des entiers relatifs.

Démontrer la propriété : ② $Y = AX + B \Rightarrow Y \wedge X = X \wedge B$.

c. En utilisant les propriétés ① et ②, montrer que : $\forall n \in \mathbb{N}, u_{n+1} \wedge a(a + 1) = 1$.

2. Établir, par récurrence, que : $\forall n \in \mathbb{N}, u_{n+1} \wedge u_n = 1$.

3. Prouver que : $\forall n \in \mathbb{N}, u_{2n+1} \equiv 0 [2a + 1]$.

4.a. Montrer que pour tous entiers α, β et γ , on a :

$$\textcircled{3} \begin{cases} \alpha \wedge \beta = 1 \\ \gamma / \alpha \end{cases} \Rightarrow \alpha \wedge (\beta\gamma) = |\gamma|$$

b. En déduire que : $\forall n \in \mathbb{N}, u_{2n+3} \wedge u_{2n+1} = 1 + 2a$.

Corrigé

1.a. Soit α, β et γ trois entiers.

Selon le théorème de Bézout :

$$\alpha \wedge \beta = 1 \Leftrightarrow \exists u, v \in \mathbb{Z} \text{ tels que } u\alpha + v\beta = 1.$$

Et

$$\alpha \wedge \gamma = 1 \Leftrightarrow \exists u', v' \in \mathbb{Z} \text{ tels que } u'\alpha + v'\gamma = 1.$$

Donc : $(u\alpha + v\beta)(u'\alpha + v'\gamma) = 1$.

Soit après développement : $(uu'\alpha + uv'\gamma + u'v\beta)\alpha + vv'(\beta\gamma) = 1$

Et donc α et $\beta\gamma$ sont premiers entre eux c'est-à-dire que $\alpha \wedge (\beta\gamma) = 1$.

b. Soit A, B, X et Y des entiers relatifs tels que $Y = AX + B$. Posons $d = Y \wedge X$ et $d' = X \wedge B$.

On a :

$$\begin{cases} d / X \\ d / Y \end{cases} \Rightarrow \begin{cases} d / X \\ d / Y - AX = B \end{cases} \text{ donc } d / d'.$$

Réciproquement :

$$\begin{cases} d' / X \\ d' / B \end{cases} \Rightarrow \begin{cases} d / X \\ d / AX + B = Y \end{cases} \text{ donc } d' / d.$$

On en déduit donc que $d = d'$.

c. Raisonnons par récurrence sur n :

Soit la propriété P_n : $\ll \forall n \in \mathbb{N}, u_{n+1} \wedge a(a+1) = 1 \gg$.

→ Initialisation :

Il s'agit de prendre $n = 0$ et d'établir donc que : $u_1 \wedge a(a+1) = 1$ c'est-à-dire que :

$$(2a+1) \wedge a(a+1) = 1.$$

Pour cela, montrons tout d'abord que : $(2a+1) \wedge a = 1$ et $(2a+1) \wedge (a+1) = 1$. On a :

$(2a+1) \wedge a = 1$ car $(2a+1) - 2a = 1$ (théorème de Bézout)

$(2a+1) \wedge (a+1) = 1$ car $2(a+1) - (2a+1) = 1$ (Idem)

Donc en vertu de la question a. : $(2a+1) \wedge a(a+1) = 1$ et par suite P_0 est vraie.

→ Transmission :

On suppose qu'il existe un rang n pour lequel P_n est vraie c'est-à-dire que : $u_{n+1} \wedge a(a+1) = 1$.

Montrons que P_{n+1} est vraie autrement dit que : $u_{n+2} \wedge a(a+1) = 1$.

On sait que : $\underbrace{u_{n+2}}_Y = \underbrace{a(a+1)}_X \underbrace{(-u_n)}_A + \underbrace{(2a+1)u_{n+1}}_B$

D'où, par application de la propriété (2) : $u_{n+2} \wedge a(a+1) = a(a+1) \wedge (2a+1)u_{n+1}$.

On sait également que :

$$(2a+1) \wedge a(a+1) = 1 \text{ (établie à l'étape de l'initialisation)}$$

et

$$u_{n+1} \wedge a(a+1) = 1 \text{ (d'après l'hypothèse de récurrence)}.$$

Donc en appliquant la propriété (1), on peut conclure que : $a(a+1) \wedge (2a+1)u_{n+1} = 1$

et par conséquent : $u_{n+2} \wedge a(a+1) = 1$. Donc P_{n+1} est vraie.

Conclusion : La propriété est vraie pour $n = 0$ et héréditaire à partir de ce rang, donc la propriété est vraie pour tout entier naturel n .

2. Soit la propriété Q_n : $\ll \forall n \in \mathbb{N}, u_{n+1} \wedge u_n = 1 \gg$.

→ Pour $n = 0$, on a : $u_0 = 2$ et $u_1 = 2a+1$ et donc $u_1 \wedge u_0 = 1$ car $2a+1$ est impair. Donc Q_0 est vraie.

→ On suppose que la propriété est vraie pour un rang donné n , c'est-à-dire que : $u_{n+1} \wedge u_n = 1$.

Montrons que la propriété est vraie pour le rang $n+1$, c'est-à-dire que : $u_{n+2} \wedge u_{n+1} = 1$.

La propriété (2) appliquée à la relation de récurrence : $u_{n+2} = (2a+1)u_{n+1} - a(a+1)u_n$ nous conduit à écrire : $u_{n+2} \wedge u_{n+1} = u_{n+1} \wedge a(a+1)u_n$.

D'autre part, comme $u_{n+1} \wedge u_n = 1$ (hypothèse de récurrence) et $u_{n+1} \wedge a(a+1) = 1$ alors la propriété (1) permet d'écrire : $u_{n+1} \wedge a(a+1)u_n = 1$. Donc on a bien : $u_{n+2} \wedge u_{n+1} = 1$.

Conclusion : La propriété Q_n est vraie pour tout entier naturel n .

3. Procédons également, dans cette question, par un raisonnement par récurrence sur n .

Soit la propriété : $\ll \forall n \in \mathbb{N}, u_{2n+1} \equiv 0 [2a+1] \gg$.

→ Pour $n = 0$, on a : $u_1 = 2a+1$ et bien entendu $u_1 \equiv 0 [2a+1]$. La propriété est vraie pour la première valeur $n = 0$.

→ On suppose que $u_{2n+1} \equiv 0 [2a+1]$ pour un rang donné n . Montrons que $u_{2n+3} \equiv 0 [2a+1]$.

En décalant les indices d'une unité, la relation de récurrence, définissant la suite (u_n) , s'écrit :

$$u_{2n+3} = (2a+1)u_{2n+2} - a(a+1)u_{2n+1}.$$

On a : $(2a+1)/u_{2n+1}$ (hypothèse de récurrence) et $(2a+1)/(2a+1)$, donc l'entier $2a+1$ divise toute combinaison linéaire de u_{2n+1} et de $(2a+1)$, et en particulier :

$(2a+1)/(2a+1)u_{2n+2} - a(a+1)u_{2n+1}$ soit $(2a+1)/u_{2n+3}$ et donc $u_{2n+3} \equiv 0 [2a+1]$.

Conclusion : la propriété est vraie pour tout entier naturel n .

4.a. Soit α, β et γ trois entiers relatifs vérifiant $\begin{cases} \alpha \wedge \beta = 1 \\ \alpha / \gamma \end{cases}$.

On sait que : $\alpha / \gamma \Rightarrow \exists k \in \mathbb{Z} \text{ tel que } \alpha = k\gamma$.

Donc, on peut alors écrire : $\alpha \wedge (\beta\gamma) = (k\gamma) \wedge (\beta\gamma) = |\gamma| \times (k \wedge \beta)$.

Posons $d = k \wedge \beta$. On a :

$$\begin{aligned} \begin{cases} d / k \\ d / \beta \end{cases} &\Rightarrow \begin{cases} d / k\gamma \\ d / \beta \end{cases} \\ \begin{cases} d / k\gamma \\ d / \beta \end{cases} &\Rightarrow \begin{cases} d / \alpha \\ d / \beta \end{cases} \end{aligned}$$

Soit enfin $d \mid (\alpha \wedge \beta)$ et donc $d = 1$, c'est-à-dire que $k \wedge \beta = 1$ et par suite $\alpha \wedge (\beta\gamma) = |\gamma|$.

b. Montrons que : $\forall n \in \mathbb{N}, u_{2n+3} \wedge u_{2n+1} = 1$.

On a, d'une part :

$$\underbrace{u_{2n+3}}_Y = (2a+1)u_{2n+2} - a(a+1)u_{2n+1} = -a(a+1)\underbrace{u_{2n+1}}_X + \underbrace{(2a+1)u_{2n+2}}_B$$

Donc la propriété ② donne : $u_{2n+3} \wedge u_{2n+1} = u_{2n+1} \wedge (2a+1)u_{2n+2}$.

D'autre part, la propriété ③ s'applique, en remarquant qu'on a simultanément :

$$u_{2n+1} \wedge u_{2n+2} = 1 \quad \text{et} \quad (2a+1)/u_{2n+1}$$

pour aboutir à : $u_{2n+1} \wedge (2a+1)u_{2n+2} = |2a+1| = 2a+1$ (car $2a+1$ est un entier naturel).

Donc enfin, nous obtenons : $u_{2n+3} \wedge u_{2n+1} = 1$.

Exercice 88

Selon les statistiques, il y a une personne sur cinq qui est déséquilibrée. S'il y a 4 personnes autour de toi qui te semblent normales, alors c'est vraiment inquiétant.

Partie I – Question de cours

- Démontrer que si p est un entier premier, alors tout naturel m tel que $1 \leq m < p$ est premier avec p .
- Démontrer que si tout entier naturel m tel que $1 \leq m < p$ est premier avec p , alors p est premier.

Partie II – La fonction indicatrice d'Euler

Pour tout entiers n supérieur ou égal à 2, on note $\varphi(n)$ le nombre d'entiers a tels que $1 \leq a < n$ et a premier avec n . Ainsi, on a : $\varphi(n) = \text{Card}\{k, k \in \mathbb{N}, 1 \leq k < n \text{ et } \text{PGCD}(k, n) = 1\}$. La fonction φ est appelée fonction indicatrice d'Euler ou parfois la fonction totient ; $\varphi(n)$ est le totient de n .

(En anglais, on parle de totient function, du latin « totiens = tant de fois », proche de « quotiens = combien de fois », mais d'usage interrogatif, qui a donné quotient en français et en anglais : chercher le quotient de n par p c'est chercher combien de fois : "il y a p dans n ".)

- Calculer les totients de 2, 3, 4, 5 et 8.
- Démontrer que : Si p est un nombre premier, alors $\varphi(p) = p - 1$.
- Soit p un nombre premier et k un entier naturel non nul. Démontrer que : $\varphi(p^k) = p^{k-1}(p - 1)$.
- Démontrer que si p et q sont premiers entre eux, alors :
 $\varphi(p \times q) = \varphi(p) \times \varphi(q)$ (On dit que φ est arithmétique).
- Démontrer que pour tout entiers $n \geq 3$, le totient $\varphi(n)$ est pair.

☞ Distinguer deux cas :

- n possède un facteur premier impair ;
- n ne possède pas un facteur premier impair.

Partie III – Application

On admet le résultat suivant appelé théorème d'Euler :

« Soit a et n deux entiers naturels. Si $\text{PGCD}(a; n) = 1$ alors $a^{\varphi(n)} \equiv 1 [n]$ ».

- Énoncer le petit théorème de Fermat et démontrer-le en utilisant le théorème d'Euler.
- a. Calculer $\varphi(2\,025)$.
- b. En déduire que $532^{1080} \equiv 1 [2\,025]$.
3. Démontrer que 72 divise $25^{24} - 1$.

Partie IV – la relation : $\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$

1. Soit d un diviseur positif de $n \in \mathbb{N}^*$. On cherche à déterminer il y a combien d'entiers k vérifiant $k \in [1, n]$ et $\text{PGCD}(k; n) = d$.

a. Soit un entier $k \in [1, n]$ tel que $\text{PGCD}(k; n) = d$. On peut écrire $n = dm$.

* Justifier que d divise k . On peut donc écrire $k = dl$.

** Montrer que $l \in [1, m]$ et que $\text{PGCD}(l; m) = 1$.

*** Inversement soit k un entier tel que $k = dl$ et $\text{PGCD}(l; m) = 1$.

Montrer : $k \in [1, n]$ et $\text{PGCD}(k; n) = d$.

b. Conclure.

2. En remarquant que :

$$[1, n] = \bigcup_{d|n} \{k \in [1, n] \text{ tel que } \text{PGCD}(k; n) = d\}$$

montrer que :

$$n = \sum_{d|n} \text{Card}\{k \in [1, n] \text{ tel que } \text{PGCD}(k; n) = d\}$$

puis que :

$$n = \sum_{d|n} \varphi(d)$$

3. Question subsidiaire

Soit n un entier naturel supérieur ou égal à 2 et $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers avec $p_1 < p_2 < \dots < p_r$ et $\forall i \in \llbracket 1, r \rrbracket, \alpha_i \geq 1$.

a. Montrer que : $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$.

b. En remarquant que $\forall i \in \llbracket 1, r \rrbracket, p_i \geq 1 + i$, établir que :

$$\left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \geq \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \dots \left(1 - \frac{1}{r+1}\right)$$

puis que $\varphi(n) \geq \frac{n}{r+1}$.

c. Justifier que $n \geq p_1 \times p_2 \times \dots \times p_r \geq 2^r$. En déduire que : $\varphi(n) \geq \frac{n \cdot \ln 2}{n + \ln 2}$.

Corrigé

Partie I

Les 2 questions découlent de la définition de nombre premier et de celle de deux entiers premiers entre eux.

Partie II

1. On a $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 4$; $\varphi(8) = 4$.

2. D'après la partie I, si p est premier alors p est premier avec tout entier m tel que $1 \leq m < p$. Donc :

$$\varphi(p) = p - 1.$$

3. Recherchons les entiers m inférieurs à p^k non premiers avec p : si $d \neq 1$ divise m et p^k , l'entier p étant premier, m est un multiple de p de la forme $d \times p < p^k$, donc $d < p^{k-1}$. Il y a donc $p^{k-1} - 1$ entiers m non premiers avec p^k . Or, $\text{Card} \{m, m \in \mathbb{N}, 1 \leq m \leq p^k - 1\} = p^k - 1$. D'où :

$$\varphi(p^k) = p^k - 1 - (p^{k-1} - 1) = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right).$$

4. Recherchons les entiers k inférieurs à pq , non premiers avec pq .

Si $d \neq 1$ divise k et pq , les entiers p et q étant premiers, k est un multiple de p ou un multiple de q , donc de la forme $d \times q < pq$ ou $d \times p < pq$. Le premier cas fournit $d < p$ ce qui conduit à $k \in \{q, 2q, \dots, (p-1)q\}$ de cardinal $p-1$. Le second cas conduit à $k \in \{p, 2p, \dots, (q-1)p\}$ de cardinal $q-1$. Or, on sait que : $\text{Card} \{k, k \in \mathbb{N}, 1 \leq k \leq pq - 1\} = pq - 1$. D'où :

$$\varphi(pq) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1) = \varphi(p) \times \varphi(q)$$

puisque p et q sont premiers.

5. Si n possède un facteur premier impair p alors on peut écrire $n = p^\alpha \times m$ avec m premier avec p .

On a alors :

$$\varphi(n) = \varphi(p^\alpha) \varphi(m) = (p^\alpha - p^{\alpha-1}) \varphi(m).$$

Puisque $p^\alpha - p^{\alpha-1}$ est un nombre pair (par différence de deux impairs), alors $\varphi(n)$ est pair. Si n ne possède pas de facteurs premiers impairs, on peut écrire $n = 2^\alpha$ avec $\alpha > 2$ et alors $\varphi(n) = 2^\alpha - 2^{\alpha-1} = 2^{\alpha-1}$ est un nombre pair.

Partie III

1. - Le petit théorème de Fermat :

« Soit n un nombre premier. Pour tout entier a non multiple de n , on a $a^{n-1} \equiv 1 [n]$ »

- Preuve à la lumière d'Euler : Comme n est premier et a entier non multiple de n alors $\text{PGCD}(a, n) = 1$. Le théorème d'Euler permet alors de conclure que $a^{\varphi(n)} \equiv 1 [n]$. Or si n est premier, $\varphi(n) = n - 1$ et par conséquent : $a^{n-1} \equiv 1 [n]$. CQFD.

2.a. En décomposant 2 025, on trouve : $2025 = 3^4 \times 5^2$. D'où : $\varphi(2025) = \varphi(3^4 \times 5^2) = \varphi(3^4) \times \varphi(5^2)$ car 3^4 et 5^2 sont premiers entre eux. D'autre part selon la question 3. de la partie II, on a :

$$\varphi(3^4) = 3^4 - 3^3 = 54 \text{ et } \varphi(5^2) = 5^2 - 5^1 = 20. \text{ Donc } \varphi(2025) = 54 \times 20 = 1080.$$

b. Il suffit de vérifier que $\text{PGCD}(2025, 532) = 1$ pour arriver au résultat escompté par application du théorème d'Euler. Dans la décomposition en facteurs premiers de 2 025 figurent seulement les facteurs premiers 3 et 5 ; et comme 532 n'est ni divisible par 3 ni par 5 alors $\text{PGCD}(2025, 532) = 1$ et la conclusion en découle.

3. On a $72 = 2^3 \times 3^2$ et donc : $\varphi(72) = \varphi(2^3 \times 3^2) = \varphi(2^3) \times \varphi(3^2) = (2^3 - 2^2)(3^2 - 3^1) = 24$.
Et comme $\text{PGCD}(72, 25) = 1$ alors Euler permet de conclure que : $a^{\varphi(72)} = 1 \pmod{25}$ et donc $a^{24} = 1 \pmod{25}$.

Partie IV

1. a. * d divise k car $d = \text{PGCD}(k; n)$. Donc il existe un entier l tel que $k = dl$.

** on a $k \leq n$ i.e. $dl \leq dm$ et donc $l \leq m$ soit $l \in \llbracket 1, m \rrbracket$. D'autre part, on a $d = \text{PGCD}(k; n) = \text{PGCD}(dl; dm) = d \times \text{PGCD}(l; m)$ et donc $\text{PGCD}(l; m) = 1$ et les entiers l et m sont premiers entre eux.

*** Inversement : Si $k = dl$ avec $l \in \llbracket 1, m \rrbracket$ et $\text{PGCD}(l; m) = 1$ alors $k \in \llbracket 1, n \rrbracket$ et $\text{PGCD}(k; n) = \text{PGCD}(dl; dm) = d \times \text{PGCD}(l; m) = d$.

b. Donc d'après la question précédente, il y a autant de k cherché que d'entiers l de $\llbracket 1, m \rrbracket$, premiers avec m , à savoir $\varphi(m)$.

2. Les ensembles $\{k \in \llbracket 1, n \rrbracket \text{ tel que } \text{PGCD}(k, n) = d\}$ étant disjoints deux à deux et que :

$$\llbracket 1, n \rrbracket = \bigcup_{d|n} \{k \in \llbracket 1, n \rrbracket \text{ tel que } \text{PGCD}(k; n) = d\}$$

$$\text{alors : } n = \text{Card} \llbracket 1, n \rrbracket = \text{Card} \left(\bigcup_{d|n} \{k \in \llbracket 1, n \rrbracket \text{ tel que } \text{PGCD}(k; n) = d\} \right)$$

$$= \sum_{d|n} \{k \in \llbracket 1, n \rrbracket \text{ tel que } \text{PGCD}(k; n) = d\} = \sum_{d|n} \varphi(d)$$

On dit que l'entier n est la somme des totients de ses diviseurs dans $\mathbb{N}$.

3. Question subsidiaire

a. L'égalité $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$ peut être établie par récurrence sur r en usant et abusant de l'arithméticité de φ car on a $\varphi(p \times q) = \varphi(p) \times \varphi(q)$ pour p et q premiers entre eux.

b. Comme on a $\forall i \in \llbracket 1, r \rrbracket, p_i \geq 1 + i$ alors $\forall i \in \llbracket 1, r \rrbracket, -\frac{1}{p_i} \geq -\frac{1}{1+i}$ et par suite :

$$\forall i \in \llbracket 1, r \rrbracket, \quad 1 - \frac{1}{p_i} \geq 1 - \frac{1}{1+i}$$

$$\text{D'où : } \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \geq \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \dots \left(1 - \frac{1}{r+1}\right) = \frac{1}{2} \times \frac{2}{3} \times \dots \times \frac{r}{r+1}.$$

$$\text{Or } \frac{1}{2} \times \frac{2}{3} \times \dots \times \frac{r}{r+1} = \frac{1}{r+1} \text{ (par télescopage). Donc : } \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \geq \frac{1}{r+1}.$$

$$\text{En multipliant par } n, \text{ on obtient : } n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \geq \frac{n}{r+1} \text{ soit l'inégalité } \varphi(n) \geq \frac{n}{r+1}.$$

c. Comme $\forall i \in \llbracket 1, r \rrbracket, \alpha_i \geq 1$ alors on a : $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \geq p_1 \times p_2 \times \dots \times p_r$. D'autre part 2 étant le plus petit entier naturel premier et les p_i des nombres premiers, on a :

$$p_1 \times p_2 \times \dots \times p_r \geq \underbrace{2 \times 2 \times 2 \times \dots \times 2}_{r \text{ facteurs égaux à } 2} = 2^r, \text{ et donc } n \geq 2^r.$$

$$* \text{ L'inégalité } \varphi(n) \geq \frac{n \ln 2}{n + \ln 2} :$$

$$n \geq 2^r \Rightarrow \ln n \geq r \ln 2 \text{ (car la fonction } x \mapsto \ln x \text{ est croissante)}$$

$$\Rightarrow \frac{n}{\ln n} \geq \frac{\ln n}{\ln n} \geq r \text{ (car } \ln 2 > 0 \text{ et } n \geq \ln n)$$

$$\Rightarrow 1 + \frac{n}{\ln 2} \geq r + 1$$

$$\Rightarrow \frac{1}{r+1} \geq \frac{1}{1 + \frac{n}{\ln 2}} = \frac{\ln 2}{n + \ln 2}$$

$$\text{Donc en multipliant par } n, \text{ on obtient } \frac{n}{r+1} \geq \frac{n \ln 2}{n + \ln 2} \text{ et par suite } \varphi(n) \geq \frac{n \ln 2}{n + \ln 2}.$$

Exercice 89

Les maths, c'est comme le sport, sauf qu'on court dans la tête.

Les nombres parfaits pairs

On dit qu'un entier naturel est parfait s'il est égal à la somme de ses diviseurs positifs autres que lui-même.

1. Le but de cette question est de montrer que si le nombre $2^p - 1$ est premier alors l'entier naturel défini par $N = 2^{p-1}(2^p - 1)$ est parfait. (Résultat dû à Euclide). Notons q l'entier $2^p - 1$.

a. Écrire la liste des diviseurs positifs de N (on remarquera que l'écriture connue de N est sa décomposition en facteurs premiers).

b. Montrer que N est parfait.

2. Preuve de la réciproque. (Résultat dû à Euler) : Soit N un nombre parfait pair. En notant n l'exposant de 2 dans la décomposition de N en facteurs premiers (N est pair, donc $n \geq 1$) on peut écrire $N = 2^n q$ avec q impair. On note : $S(N)$ la somme des diviseurs de N (N est parfait, donc $S(N) = 2N$) et $S(q)$ la somme des diviseurs de q .

a. En remarquant que chaque diviseur d de q engendrent $n + 1$ diviseurs de N , montrer que :

$$S(N) = (1 + 2 + 2^2 + \dots + 2^n) \times S(q) \text{ puis que : } 2N = (2^{n+1} - 1) \times S(q).$$

b. En notant σ la somme des diviseurs de q autres que q , déduire de 2.a. que : $q = \sigma(2^{n+1} - 1)$.

c. En déduire que $\sigma = 1$, puis que q est premier et égal à $2^{n+1} - 1$. Ainsi $N = 2^n(2^{n+1} - 1)$.

Corrigé

1.a. Notons $q = 2^p - 1$; on suppose que q est premier, donc $2^{p-1} \times q$ est la décomposition en facteurs premiers de N , donc N admet $p \times 2$ diviseurs : $1 ; 2 ; 2^2 ; \dots ; 2^{p-1}$ et $q ; 2q ; 2^2q ; \dots ; 2^{p-1}q$.

b. La somme des diviseurs positifs de N autres que lui-même est :

$$\begin{aligned} 1 + 2 + 2^2 + \dots + 2^{p-1} + q + 2q + 2^2q + \dots + 2^{p-2}q &= \frac{2^p - 1}{2 - 1} + q \frac{2^{p-1} - 1}{2 - 1} \\ &= 2^p - 1 + (2^p - 1)(2^{p-1} - 1) \\ &= (2^p - 1) \times 2^{p-1} = N. \end{aligned}$$

Donc N est parfait.

2. a. Les diviseurs de N sont $1 ; 2 ; 2^2 ; \dots ; 2^n$ et, pour tout diviseur $d \neq 1$ de q ; $d ; 2d ; 2^2d ; \dots ; 2^nd$; donc $S(N) = (1 + 2 + 2^2 + \dots + 2^n) \times S(q)$. Comme $S(N) = 2N$ et $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$, alors on a : $2N = (2^{n+1} - 1) \times S(q)$.

$$b. 2N = (2^{n+1} - 1) \times S(q) \Leftrightarrow 2^{n+1}q = (2^{n+1} - 1) \times (\sigma + q)$$

$$\Leftrightarrow 0 = (2^{n+1} - 1)\sigma - q \Leftrightarrow q = \sigma(2^{n+1} - 1)$$

c. D'après la question précédente, σ divise q et $\sigma < q$ (car $n \geq 1$), donc σ est un des termes de la somme égale à σ , donc σ est le seul terme de cette somme, donc $\sigma = 1$. Alors, les diviseurs de q sont 1 et q , donc q est premier. L'égalité de la question 2.b. s'écrit : $q = 2^{n+1} - 1$. D'où $N = 2^n(2^{n+1} - 1)$.

Conclusion : tous les nombres parfaits pairs sont de la forme $2^{p-1}(2^p - 1)$ avec $2^p - 1$ premier.

Exercice 90

Si le crocodile achète un pantalon, c'est qu'il a trouvé où mettre sa queue.

1. Montrer que, si n est un entier naturel impair non premier, alors il existe des entiers naturels impairs k et d tels que : $n = kd$; $1 < d < n$; $1 < k < n$.

2. En 1934, le mathématicien indien **Sundaram** proposa un crible pour obtenir les entiers premiers impairs : Partant de l'entier 4 : on construit en lignes et en colonnes les termes des suites arithmétiques dont les raisons sont les entiers impairs successifs 3, 5, 7, 9, ...

La propriété de Sundaram dit : « un entier impair $2k + 1$ différent de 1 est premier si, l'entier non nul k ne figure pas dans ce tableau ».

Montrons cette propriété.

On note $a_{i,j}$ le terme du tableau situé à l'intersection de la ligne i et de la colonne j .

a. La colonne 1 étant constituée des termes d'une suite arithmétique de raison 3, exprimer $a_{i,1}$ en fonction de i .

b. La ligne i est constituée des termes d'une suite arithmétique ; exprimer sa raison en fonction de i .

c. En déduire que $a_{i,j} = i + j + 2ij$.

d. Vérifier que $2a_{i,j} + 1 = (2i + 1)(2j + 1)$.

e. Conclure

4	7	10	13	...
7	12	17	22	...
10	17	24	31	...
13	22	31	40	...
...	...	...	...	...

Corrigé

1. Comme n n'est pas premier, il existe des entiers k et d tels que :

$n = kd$; $1 < k < n$; $1 < d < n$. De plus n étant impair, k et d sont impairs sinon kd serait pair.

2.a. on a : $a_{i,1} = 4 + 3(i - 1) = 3i + 1$ (suite arithmétique de raison 3 et de 1^{er} terme $a_{1,1} = 4$).

- b. La raison est $r_i = 3 + 2(i - 1) = 2i + 1$ (les entiers impairs à partir de 3).
- c. Sur la ligne i , on sait que la suite $(a_{i,j})$ est une suite arithmétique de raison r_i et de 1^{er} terme $a_{i,1}$ et donc :
- $$a_{i,j} = a_{i,1} + (j - 1)r_i = 3i + 1 + (j - 1)(2i + 1) = 3i + 1 + 2ij + j - 2i - 1 = i + j + 2ij$$
- d. On a : $(2i + 1)(2j + 1) = 4ij + 2i + 2j + 1 = 2a_{i,j} + 1$.
- e. Si k figure dans le tableau, le résultat précédent montre clairement que $2k + 1$ n'est pas premier. Réciproquement, si k ne figure pas dans le tableau, alors $2k + 1$ est premier sinon, d'après la question précédente $2k + 1$ serait le produit de deux entiers impairs autres que 1 et $2k + 1$; ces deux entiers impairs seraient de la forme $2i + 1$ et $2j + 1$ avec $i \geq 1$ et $j \geq 1$, donc $k = a_{i,j}$ serait dans le tableau.

Exercice 91

On est plus le fils de son époque que le fils de son père.

Calcul sur le calendrier grégorien

On se propose de trouver le jour de la semaine associé à une date donnée.

Pour cela, on utilise le calendrier depuis le 20 décembre 1582. On rappelle que le mois de février compte 29 ou 28 jours, selon que l'année est bissextile ou non. Une année est bissextile lorsque son millésime A est un multiple de 400 ou lorsque A est un multiple de 4 sans être un multiple de 100 (ainsi 1900 n'est pas bissextile).

1. a et b désignent deux entiers naturels avec $b \neq 0$, q est le quotient de la division de a par b .

Démontrer que $q = E\left(\frac{a}{b}\right)$ où $E(x)$ désigne la partie entière de x .

2. On note B le nombre d'années bissextiles qui ont précédé strictement au 1^{er} janvier de l'année A depuis la date fictive du 1^{er} janvier de l'an 1 (qui va nous servir d'origine des dates).

a. Démontrer que : $B = E\left(\frac{A-1}{4}\right) - E\left(\frac{A-1}{100}\right) + E\left(\frac{A-1}{400}\right)$.

b. Démontrer que le nombre N de jours dans les années qui précèdent à l'année A est donnée par :

$$N = B + 365(A - 1).$$

c. On note $(J; M; A)$ une date : J entre 1 et 31, M entre 1 et 12, A l'année (avec $A \geq 1582$).

Comment calculer le nombre R de jours entre les dates $(1; 1; A)$ et $(J; M; A)$ (ces deux jours compris).

d. Le nombre N de jours entre les dates $(1; 1; 1)$ et $(J; M; A)$ est donc donné par : $N = R + B + 365(A - 1)$.

Vérifier que $N \equiv A - 1 + B + R \pmod{7}$.

e. En sachant que le 1^{er} janvier 2003 est un mercredi, vérifier que le nombre N associé à mercredi 1^{er} janvier 2003 vérifie $N \equiv 3 \pmod{7}$.



دستار المختار ولد داداه
مختار موكhtar Ould Daddah
IDENT DE LA REPUBLIQUE ISLAMIQUE DE MAURITANIE

3.a. A la suite du vote de la Loi-Cadre Defferre par l'Assemblée Nationale française le 23 juin 1956, loi qui ouvre la voie à l'autonomie des anciennes colonies, Mokhtar OULD DADDAH (photo ci-contre) est élu conseiller territorial le 31 mars 1957, puis vice-président du Conseil de Gouvernement le 20 mai de la même année. Il prononce alors son célèbre appel « Faisons ensemble la patrie mauritanienne ». Le 24 mai 1957, Mokhtar OULD DADDAH réunit à Saint-Louis le premier Conseil de Gouvernement, car la Mauritanie n'a pas encore de capitale sur son territoire. Dès son installation, il plaide pour la création d'une capitale sur le territoire national ce sera Nouakchott, petit fort militaire créé par les Français au début du XX^{ème} siècle, et situé au sud-ouest du pays sur la piste impériale reliant Casablanca à Dakar, à 4 kilomètre de la

mer.

Le 28 novembre 1960, Mokhtar OULD DADDAH, en présence de nombreuses délégations étrangères, proclame solennellement l'Indépendance de la République Islamique de Mauritanie. Quel jour de la semaine était ce 28 novembre 1960?



Karl Friedrich
Gauss
(1777-1855)

b. Quel jour de la semaine était né le prince des mathématiques Carl Friedrich Gauss sachant qu'il est né le 30 avril 1777 à Brunswick (en Allemagne)?



Etienne Bézout
(1730-1783)

c. Faire de même pour notre incontournable secours en Arithmétique, le mathématicien français Etienne Bézout sachant qu'il est né le 31 mars 1730.

Corrigé

1. a et b désignent deux entiers naturels avec $b \neq 0$, q est le quotient de la division euclidienne de a par b donc il existe un entier naturel r tel que $0 \leq r < b$ et $a = bq + r$ donc $\frac{a}{b} = q + \frac{r}{b}$ et $0 \leq \frac{r}{b} < 1$ donc $q \leq \frac{a}{b} < q + 1$, donc $q = E\left(\frac{a}{b}\right)$.

2. a. Entre le 1er janvier de l'année A et le 1er janvier de l'an 1, se sont déroulées $A - 1$ années. En effectuant la division euclidienne de $A - 1$ par 4, il existe deux entiers naturels q et r tels que $A - 1 = 4q + r$ avec $0 \leq r < 4$. Il y a donc $q = E\left(\frac{A-1}{4}\right)$, il existe donc $E\left(\frac{A-1}{4}\right)$ multiples de 4 compris entre A et 1. De même il existe $E\left(\frac{A-1}{100}\right)$ multiples de 100 compris entre A et 1.

Le nombre $E\left(\frac{A-1}{4}\right) - E\left(\frac{A-1}{100}\right)$ est le nombre des multiples de 4 qui ne sont pas multiples de 100 (les multiples de 400 sont donc exclus). Il existe $E\left(\frac{A-1}{400}\right)$ multiples de 400 compris entre A et 1 donc le nombre d'années bissextiles comprises entre 1 et A est :

$$B = E\left(\frac{A-1}{4}\right) - E\left(\frac{A-1}{100}\right) + E\left(\frac{A-1}{400}\right).$$

b. Pendant $A - 1$ années se sont déroulés $(A - 1) \times 365$ jours auxquels on doit ajouter les B jours additionnels des années bissextiles donc le nombre N de jours dans les années qui précèdent à l'année A est donné par : $N = B + 365(A - 1)$.

c. Entre $(1; 1; A)$ et $(1; M; A)$ se sont déroulés si A n'est pas une année bissextile :

Mois	Janv.	Fév.	Mars	Avril	Mai	Juin
R	1	32	60	91	121	152

Mois	Juillet	Août	Sept.	Oct.	Nov.	Déc.
R	182	213	244	274	305	335

Entre $(J; M; A)$ et $(1; 1; A)$

Mois	Janv.	Fév.	Mars	Avril	Mai	Juin
R	J	$31 + J$	$59 + J$	$90 + J$	$120 + J$	$151 + J$

Mois	Juillet	Août	Sept.	Oct.	Nov.	Déc.
R	$181 + J$	$212 + J$	$243 + J$	$273 + J$	$304 + J$	$334 + J$

Entre $(1; 1; A)$ et $(1; M; A)$ se sont déroulés si A est une année bissextile :

Mois	Janvier	Fév.	Mars	Avril	Mai	Juin
R	1	32	61	92	122	153

Mois	Juillet	Août	Sept.	Oct.	Nov.	Déc.
R	183	214	245	275	306	336

Entre $(J; M; A)$ et $(1; 1; 1)$

Mois	Janv.	Fév.	Mars	Avril	Mai	Juin
R	J	$31 + J$	$60 + J$	$91 + J$	$121 + J$	$152 + J$

Mois	Juillet	Août	Sept.	Oct.	Nov.	Déc.
R	$182 + J$	$213 + J$	$244 + J$	$274 + J$	$305 + J$	$335 + J$

d. Le nombre N de jours entre les dates $(1; 1; 1)$ et $(J; M; A)$ est donc : $N = R + B + 365(A - 1)$ et comme on sait que : $365 = 7 \times 52 + 1$ càd $365 \equiv 1 [7]$ alors :

$$R + B + 365(A - 1) \equiv R + B + A - 1 [7] \text{ donc } N \equiv A - 1 + B + R [7].$$

e. En sachant que le 1er janvier 2003 est un mercredi, vérifier que le nombre N associé à mercredi 1er janvier 2003 vérifie : $N \equiv 3 [7]$.

$$B = E\left(\frac{2003-1}{4}\right) - E\left(\frac{2003-1}{100}\right) + E\left(\frac{2003-1}{400}\right) = 500 - 20 + 5 = 485 \text{ et } R = 1$$

$$N = 2003 - 1 + E\left(\frac{2003-1}{4}\right) - E\left(\frac{2003-1}{100}\right) + E\left(\frac{2003-1}{400}\right) + 1 \\ = 2003 + 485 = 2488, \text{ or } 2488 = 7 \times 355 + 3 \text{ donc } N \equiv 3 [7]$$

3.a. Entre le $(1; 1; 1)$ et le $(28; 11; 1960)$ il y a eu :

$$E\left(\frac{1960-1}{4}\right) - E\left(\frac{1960-1}{100}\right) + E\left(\frac{1960-1}{400}\right) = 474 \text{ années bissextiles.}$$

1960 est une année bissextile donc $R = 305 + 28 = 333$.

Le nombre N de jours entre les dates $(1; 1; 1)$ et $(28; 11; 1960)$ est : $N = 475 + 365 \times 1959 + 333$.

Donc $N \equiv 474 + 1959 + 333 [7]$ car $365 \equiv 1 [7]$ soit $N \equiv 2766 [7]$, or $2766 = 7 \times 395 + 1$ donc $N \equiv 1 [7]$ et enfin le 28 novembre 1960 était un lundi.

b. Entre le $(1; 1; 1)$ et le $(30; 4; 1777)$ il y a eu :

$$E\left(\frac{1777-1}{4}\right) - E\left(\frac{1777-1}{100}\right) + E\left(\frac{1777-1}{400}\right) = 431 \text{ années bissextiles.}$$

1777 n'est pas une année bissextile donc $R = 90 + 30 = 120$.

Le nombre N de jours entre les dates $(1; 1; 1)$ et $(30; 4; 1777)$ est : $N = 431 + 365 \times 1776 + 120$.

Donc $N \equiv 431 + 1776 + 120 [7]$ car $365 \equiv 1 [7]$ soit $N \equiv 2327 [7]$, or $2327 = 7 \times 332 + 3$ donc $N \equiv 3 [7]$ et enfin le 30 avril 1777 était un mercredi.

c. Entre le $(1; 1; 1)$ et le $(31; 3; 1730)$ il y a eu :

$$E\left(\frac{1730-1}{4}\right) - E\left(\frac{1730-1}{100}\right) + E\left(\frac{1730-1}{400}\right) = 419 \text{ années bissextiles.}$$

1730 n'est pas une année bissextile donc $R = 59 + 31 = 90$.

Le nombre N de jours entre les dates $(1; 1; 1)$ et $(30; 4; 1730)$ est : $N = 419 + 365 \times 1729 + 90$.

Donc $N \equiv 419 + 1729 + 90 [7]$ car $365 \equiv 1 [7]$ soit $N \equiv 2238 [7]$, or $2238 = 7 \times 319 + 5$ donc $N \equiv 5 [7]$ donc le 31 mars 1730 était un vendredi.

Exercice 92

Le vieux se chauffe avec le bois récolté dans sa jeunesse.

Une élégante démonstration de l'infinité des nombres premiers

La démonstration du théorème « l'ensemble des nombres premiers est infini » qui figure dans presque tous les manuels scolaires date d'environ 2 300 ans et a été proposée la première fois par l'honorable Euclide. Celle que nous allons voir dans cet exercice a été proposée, tout récemment, en 1938.

Supposons qu'il existe un nombre fini A d'entiers premiers que nous noterons $p_1, p_2, \dots, p_A$.

Soit N un entier supérieur ou égal à 1 et soit n un entier compris entre 1 et N .

1. En utilisant le théorème de la décomposition en facteurs premiers, justifier que n admet une écriture de la forme : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_A^{\alpha_A}$ où $\alpha_1, \alpha_2, \dots, \alpha_A$ sont des naturels éventuellement nuls.

2. On écrit chacun des exposants α_i sous la forme $2\alpha_i + b_i$, avec $b_i = 0$ si α_i est pair et $b_i = 1$ si α_i est impair. Montrer qu'on peut mettre n sous la forme : $n = k^2 \times p_1^{b_1} \times p_2^{b_2} \times \dots \times p_A^{b_A}$ où k est un entier naturel dont on précisera la valeur.

3.a. Montrer que $k^2 \leq N$.

b. Justifier qu'il y a au plus 2^A entiers de la forme : $p_1^{b_1} \times p_2^{b_2} \times \dots \times p_A^{b_A}$.

c. En déduire que le nombre de valeurs prises par n (c'est-à-dire N) est inférieur ou égal à $\sqrt{N} \times 2^A$, puis que $N \leq 2^{2A}$.

4. Conclure.

☞ N est au départ un entier quelconque.

Corrigé

1. En attribuant l'exposant zéro aux nombres premiers qui ne figurent pas dans sa décomposition, n aura une écriture de la forme : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_A^{\alpha_A}$

2. On a $n = p_1^{2a_1+b_1} \times p_2^{2a_2+b_2} \times \dots \times p_A^{2a_A+b_A} = k^2 \times p_1^{b_1} \times p_2^{b_2} \times \dots \times p_A^{b_A}$
avec $k = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_A^{a_A}$.

3.a. $k^2 \leq n \leq N$.

b. On a deux choix possibles pour chaque b_i (0 ou 1), donc il y a 2^A écritures possibles pour l'entier :

$$p_1^{b_1} \times p_2^{b_2} \times \dots \times p_A^{b_A}.$$

c. On a : $k \leq \sqrt{N}$, donc, pour écrire n , il y a au plus $\sqrt{N}$ choix possibles pour k .

Le nombre d'écritures possibles de n est donc inférieur ou égal à $\sqrt{N} \times 2^A$.

Or, par définition de n , l'entier n peut prendre N valeurs (1 ; 2 ; ... ; N).

Ainsi $N \leq \sqrt{N} \times 2^A$, ou encore $N \leq 2^{2A}$.

4. On vient de montrer que s'il y avait un nombre fini d'entiers naturels premiers, alors tout entier naturel N est inférieur ou égal à 2^{2A} autrement qu'il y aurait un nombre fini d'entiers naturels !

Exercice 93

L'amour et la haine sont un voile devant les yeux: l'un ne laisse voir que le bien, l'autre que le mal.

Nombres de Fermat – Infinitude des nombres premiers

1. Soit $a \in \mathbb{N}$. Montrer que, pour tout $k \in \mathbb{N}^*$, $(a-1)^{2^k} + 1 \equiv 2 \pmod{a}$.

2. Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (F_n est appelé le $n^{\text{ième}}$ nombre de Fermat).

Montrer que, pour tout $k \in \mathbb{N}^*$, $(F_n - 1)^{2^k} + 1 = F_{n+k}$.

En déduire qu'il existe $q \in \mathbb{N}$, tel que $F_{n+k} = qF_n + 2$.

3.a. Soient n et m deux entiers naturels, $n \neq m$. Montrer que si d est un entier naturel qui divise à la fois F_n et F_m , alors $d = 1$. En déduire que F_n et F_m sont premiers entre eux (le théorème de Goldbach).

b. En déduire que l'ensemble des nombres premiers est infini.

Corrigé

1. Soit $a \in \mathbb{N}$, $k \in \mathbb{N}^*$.

On peut développer $(a-1)^{2^k}$ par la formule du binôme de Newton : $(a-1)^{2^k}$

$$= \sum_{i=0}^{i=2^k} C_{2^k}^i a^i (-1)^{2^k-i}$$

Le seul terme qui ne contient pas a comme facteur est celui qui correspond à $i = 2^k$: il vaut 1. Donc :

$$(a-1)^{2^k} \equiv 1 \pmod{a}$$

Comme la congruence est compatible avec l'addition, il vient : $(a-1)^{2^k} + 1 \equiv 2 \pmod{a}$

2. Soit $F_n = 2^{2^n} + 1$.

Donc $F_n - 1 = 2^{2^n}$ et $(F_n - 1)^{2^k} = (2^{2^n})^{2^k} = 2^{2^{n+k}} = F_{n+k} - 1$. D'où : $(F_n - 1)^{2^k} + 1 = F_{n+k}$

La relation démontrée dans la première question montre alors, pour $a = F_n$: $F_{n+k} \equiv 2 \pmod{F_n}$.

Or l'application de $\mathbb{N}$ dans $\mathbb{N}$ qui, à un entier naturel n associe le nombre de Fermat correspondant F_n est une application croissante : $n \leq m \Rightarrow F_n \leq F_m$, donc, pour $k \in \mathbb{N}^*$, F_{n+k} est supérieur à F_n .

La relation $F_{n+k} \equiv 2 \pmod{F_n}$ montre alors qu'il existe un entier naturel $q \in \mathbb{N}$ tel que :

$$F_{n+k} = qF_n + 2.$$

3. a. Soit d un diviseur commun à F_n et à F_m , avec $n \neq m$.

On peut supposer, pour fixer les idées, que m est plus grand que n .

Posons $k = m - n$. Donc $k \in \mathbb{N}^*$. Le résultat précédent s'applique : il existe un entier naturel $q \in \mathbb{N}$ tel que : $F_{n+k} = qF_n + 2$. On a : d divise F_n , d divise F_m , donc d divise $F_m - qF_n = 2$.

2 est premier : les seuls diviseurs de 2 sont 1 et 2. Comme d ne peut pas être égal à 2 parce que les

nombre de Fermat sont impairs, ce sont des multiples de 2 plus 1 alors $d = 1$. Donc deux nombres de Fermat différents sont premiers entre eux.

b. On raisonne par l'absurde :

Supposons qu'il n'existe que n entiers premiers ($n \geq 2$).

Considérons les $n + 1$ nombres de Fermat $F_1, F_2, \dots, F_n, F_{n+1}$. On sait que chacun des F_i , où $i \in \llbracket 1; n + 1 \rrbracket$, admet un diviseur **premier** d_i . Tous les d_i sont distincts deux à deux. En effet, si pour $i \neq j$ dans $\llbracket 1; n + 1 \rrbracket$, on a $d_i = d_j$ alors F_i et F_j sont deux nombres de Fermat différents admettant un diviseur premier commun et donc ils ne sont pas premiers entre eux ; ce qui contredit le résultat de la question 3.a.

Exercice 94	Deux choses ne s'apprécient que quand on les a plus: la santé et la jeunesse.
--------------------	--

On souhaite montrer qu'il existe une infinité de nombres premiers de la forme $4k + 1$.

Supposons qu'il n'y en a qu'un nombre fini : $p_1 < p_2 < \dots < p_n$ et considérons p un diviseur premier de $N = M^2 + 1$ où $M = p_1 \cdot p_2 \dots p_n$.

1. Vérifier que $p = 2$ ou $p \equiv -1 \pmod{4}$.

2. Montrer que N admet au moins un diviseur premier p tel que $p \equiv -1 \pmod{4}$.

3.a. Si $p \equiv -1 \pmod{4}$, on peut écrire $p = 4m + 3$. Montrer que :

$$M^{p-1} - 1 = M^2(M^2 - 1)(M^2 + 1) \left(\sum_{k=0}^{m-1} M^{4k} \right) + M^2 - 1.$$

b. Montrer que p divise $M^2 - 1$.

c. En déduire que $p = 2$ puis conclure.

Corrigé

1. Si $p \equiv 1 \pmod{4}$, alors p est égale à l'un des p_i . Dans ce cas, p divise M^2 et on a :

$$p \text{ divise } N = M^2 + 1 \Rightarrow p \text{ divise } 1.$$

Impossible, donc $p = 2$ ou $p \equiv 3 \pmod{4} \equiv -1 \pmod{4}$.

2. Si aucun diviseur premier de N ne vérifie $p \equiv -1 \pmod{4}$, on peut écrire :

$$N = M^2 + 1 = 2^k \text{ avec } k \geq 2 \Rightarrow M^2 + 1 \equiv 0 \pmod{4} \Rightarrow M^2 \equiv -1 \pmod{4}.$$

Or : $M = p_1 p_2 \dots p_n \equiv 1 \pmod{4} \Rightarrow M^2 \equiv 1 \pmod{4}$

Donc $1 \equiv -1 \pmod{4}$ soit $2 \equiv 0 \pmod{4}$, ce qui est contradictoire.

3. a. Calculons :

$$\begin{aligned} M^{p-1} - 1 &= M^{4m+2} - 1 = M^2[M^{4m} - 1] + M^2 - 1 = M^2[(M^4)^m - 1] + M^2 - 1 \\ &= M^2(M^4 - 1) \sum_{k=0}^{m-1} M^{4k} + M^2 - 1 = M^2(M^2 - 1)(M^2 + 1) \sum_{k=0}^{m-1} M^{4k} + M^2 - 1. \end{aligned}$$

b. D'après le petit théorème de Fermat, on a :

$$M^{p-1} \equiv 1 \pmod{p} \Rightarrow M^{p-1} - 1 \equiv 0 \pmod{p} \Rightarrow p \text{ divise } M^{p-1} - 1.$$

Comme p divise $M^{p-1} - 1$ et $N = M^2 + 1$, p divise $M^2 - 1$ d'après cette égalité.

c. L'entier p divise $M^2 + 1$ et $M^2 - 1$, donc p divise la différence $2 = M^2 + 1 - (M^2 - 1)$ et on en déduit que $p = 2$. Il y a là contradiction avec $p \equiv -1 \pmod{4}$.

Exercice 95	La preuve est une idole devant laquelle le mathématicien se torture.
--------------------	---

1. On pose $A = 2017! + 1$.

Montrer que pour tout entier n tel que $1 \leq n \leq 2016$, le nombre $A + n$ n'est pas premier. En déduire 2016 entiers consécutifs parmi lesquels aucun n'est premier.

2. Existe-t-il une liste de mille milliards d'entiers consécutifs ne comportant aucun nombre premier ?

Remarque : Ce résultat semble témoigner de la raréfaction des nombres premiers. Cependant, une conjecture du mathématicien français Joseph Bertrand (1822-1900) démontrée par son confrère russe Pafnouti Tchebychev (1821-1894) tempère cette impression : « Si $n \geq 3$, il y a toujours un nombre premier compris entre n et $2n$ »

Corrigé

1. Pour tout entier naturel n tel que $1 \leq n \leq 2016$, on a : $A + n = 2017! + (n + 1)$ avec donc $2 \leq n + 1 \leq 2017$. L'entier $n + 1 \geq 2$ étant un facteur de $2017!$, alors :

$$n + 1 \text{ divise } 2017! + (n + 1) = A + n.$$

Donc les 2016 entiers consécutifs $A + 1, A + 2, A + 3, \dots, A + 2016$ sont tous non premiers.

2. Mille milliards s'écrit 10^{12} ($= 1000 \times 10^9$).

On pose, dans ce cas, $A = (10^{12} + 1)! + 1$. Comme dans la question précédente, on sait que les entiers $A + n$ avec $1 \leq n \leq 10^{12}$ sont tous non premiers. D'où la conclusion.

Exercice 96

Celui qui confesse son ignorance la montre une fois ; celui qui essaye de la cacher la montre plusieurs fois.

On note : $2 = p_1 < p_2 < \dots < p_n < p_{n+1} < \dots$ la suite infinie des nombres premiers rangée dans l'ordre croissant et $\pi(x)$ le nombre d'entiers premiers plus petits que x .

1. Montrer que : $\forall n \geq 1, 2n - 1 \leq p_n \leq 2^{2^{n-1}}$

2. En déduire que : $\pi(x) > \ln(\ln(x))$.

Corrigé

1. On procède par récurrence sur $n \geq 1$.

Pour $n = 1$ et $n = 2$, le résultat est évident.

On le suppose acquis pour tout entier k compris entre 1 et $n \geq 2$. Comme pour $n \geq 2$, p_n est impair, l'entier $p_n + 1$ est pair donc non premier et $p_{n+1} \geq p_n + 2$. Avec l'hypothèse de récurrence, on déduit donc que : $p_{n+1} \geq p_n + 2 \geq 2n + 1$.

Si p est un diviseur premier du produit $p_1 \dots p_n + 1$; on a nécessairement $p \geq p_{n+1}$ (sinon $p = p_k$ où k est compris entre 1 et n ; donc p divise $p_1 \dots p_n$ et 1; ce qui est impossible).

On a donc : $p_{n+1} \leq p \leq p_1 \dots p_n + 1 \leq 2^1 \times \dots \times 2^{2^{n-1}} + 1$

soit : $p_{n+1} \leq 2^{1+2+\dots+2^{n-1}} + 1 = 2^{2^n - 1} + 1 \leq 2^{2^n}$

2. Pour tout réel $x \geq 2$; la partie entière m de $\ln(\ln(x))$ est telle que :

$$-1 \leq m \leq \ln(\ln(x)) < m + 1$$

et l'entier naturel $n = m + 1$ est tel que : $n - 1 \leq \ln(\ln(x)) < n$, ce qui équivaut à :

$$e^{e^{n-1}} \leq x < e^{e^n}.$$

La fonction π étant intuitivement croissante, on a $n = \pi(p_n) \leq \pi(2^{2^{n-1}}) \leq \pi(e^{e^{n-1}}) \leq \pi(x)$.

Soit : $\pi(x) \geq n > \ln(\ln(x))$

Exercice 97

On apprend peu par la victoire, mais beaucoup par la défaite.

Problème dit de la progression arithmétique

Le mathématicien allemand Dirichlet (1805-1859) a démontré que si deux entiers naturels a et b sont premiers entre eux, alors il existe une infinité de nombres premiers de la forme $an + b$ où n est un entier naturel (résultat connu sous le nom du problème de la progression arithmétique). Mais la démonstration de ce résultat est hors de portée d'un élève de la classe de 7^{ème} C.

Dans cet exercice, on se limite à étudier un cas particulier c'est-à-dire qu'on se propose de montrer qu'il existe une infinité de nombre premiers de la forme $6k + 5$.

1. Montrer que tout nombre premier autre que 2 et 3 est de la forme $6k + 1$ ou $6k + 5$.

2. On forme l'hypothèse (H) selon laquelle il n'existe qu'un nombre fini de nombre premiers de la forme $6k + 5$ que l'on nomme $p_1 ; p_2 ; \dots ; p_n$. On considère alors l'entier $N = 6 p_1 \times p_2 \times \dots \times p_n - 1$.

a. Justifier que $N \equiv -1 \pmod{6}$.

b. En déduire que N est de la forme $6k + 5$ avec $k \in \mathbb{N}$, puis qu'il ne peut pas être premier.

c. Montrer qu'aucun des nombres $p_1 ; p_2 ; \dots ; p_n$ ne divise N et en déduire que les diviseurs premiers de N sont de la forme $6k + 1$, avec $k \in \mathbb{N}$. Montrer alors que $N \equiv 1 \pmod{6}$. Conclure.

Corrigé

1. Montrons que tout nombre premier autre que 2 et 3 est de la forme $6k + 1$ ou $6k + 5$. Soit n un entier quelconque différent de 2 et de 3, on sait alors que n est de l'une des six formes suivantes : $6k ; 6k + 1 ; 6k + 2 ; 6k + 3 ; 6k + 4 ; 6k + 5$ où $k \in \mathbb{N}$.

Si n est premier on peut exclure les cas $6k$, $6k + 2$ et $6k + 4$ divisible par 2 (2 étant exclu) et $6k + 3$ divisible par 3 (3 étant exclu). Reste donc les cas $6k + 1$ et $6k + 5$. Ainsi tout nombre premier différent de 2 et de 3 est de l'une des deux formes $6k + 1$ ou $6k + 5$.

2. On forme l'hypothèse (H) selon laquelle il existe un nombre fini de nombres premiers de la forme $6k + 5$ que l'on nomme $p_1 ; p_2 ; \dots ; p_n$ et que l'on peut supposer rangés dans l'ordre croissant, c'est à dire que $p_1 < p_2 < \dots < p_n$. On considère alors l'entier $N = 6 p_1 \times p_2 \times \dots \times p_n - 1$

a. Justifions que $N \equiv -1 [6]$

On sait que $6 p_1 \times p_2 \times \dots \times p_n \equiv 0 [6]$ donc que $N \equiv -1 [6]$.

b. Puisque $N \equiv -1 [6]$ on peut en déduire que $N \equiv 5 [6]$ donc que $N - 5$ est divisible par 6 donc qu'il existe un entier k tel que $N - 5 = 6k$ soit encore que $N = 6k + 5$.

L'hypothèse (H) nous dit qu'il existe un nombre fini de nombres premiers de la forme $6k + 5$.

On sait que p_k est strictement supérieur à 2 pour tout $k \in \{1 ; 2 ; \dots ; n\}$, on en déduit que $6 p_1 \times p_2 \times \dots \times p_n \geq 6 p_n$. On tire alors que $N > p_n$ quelque soit $k \in \{1 ; 2 ; \dots ; n\}$ et donc ne peut pas faire partie de la liste des p_k .

Donc que N ne peut être un nombre premier car il est de la forme $6k + 5$.

Une autre démonstration consiste à raisonner pas l'absurde en supposant que N est bien premier.

Comme il est de la forme $6k + 5$, c'est que c'est l'un des p_k . Cependant si on note que $N = p_k$ alors on peut dire que p_k divise N mais divise aussi le produit $p_1 \times p_2 \times \dots \times p_n$.

Par conséquent on aurait que p_k divise $N - 6 p_1 \times p_2 \times \dots \times p_n$ soit p_k divise l'entier 1, ce qui est manifestement impossible puisque p_k est un nombre premier.

c. Montrons qu'aucun de nombres $p_1 ; p_2 ; \dots ; p_n$ ne divise N .

Comme vu précédemment p_k ne peut diviser N et ce quelque soit l'entier naturel $k \in \{1 ; 2 ; \dots ; n\}$.

Mais rédigeons une démonstration.

Raisonnons pas l'absurde en supposant qu'il existe un indice k de l'ensemble $\{1 ; 2 ; \dots ; n\}$ tel que p_k divise N . Il est clair dans ces conditions que l'on a : $p_k \mid p_1 \times p_2 \times \dots \times p_n$ et $p_k \mid N$ donnent que $p_k \mid N - p_1 \times p_2 \times \dots \times p_n$ donc que $p_k \mid 1$ ce qui est absurde puisque p_k est un nombre premier.

Finalement on en déduit qu'aucun des p_k , pour $k \in \{1 ; 2 ; \dots ; n\}$, ne divise N .

Déduisons en que les diviseurs premiers de N sont de la forme $6k + 1$, avec k entier naturel. On sait que N admet une décomposition en produit de facteurs premiers de la forme $N = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_m^{\alpha_m}$ avec $m \geq 1$ et $q_1 ; q_2 ; \dots ; q_m$ des entiers premiers et $\alpha_1 ; \alpha_2 ; \dots ; \alpha_m$ des entiers non nuls.

Pour $i \in \{1 ; 2 ; \dots ; m\}$ on sait que $q_i \notin \{p_1 ; p_2 ; \dots ; p_n\}$ car si tel était le cas on aurait l'un des p_k qui serait un diviseur de N ce qui n'est pas le cas. De fait tous les q_i sont de la forme :

$$6k + 1 \text{ ou } q_i = 2 \text{ ou } q_i = 3.$$

Rappelons qu'un nombre premier différent de 2 et de 3 ne peut être que de la forme $6k + 1$ ou $6k + 5$ et l'on vient de montrer que ces nombres premiers ne peuvent pas être de la forme $6k + 5$. Or il est clair que ni 2 ni 3 ne divise N .

En effet si $2 \mid N$ alors comme $2 \mid 6 p_1 \times p_2 \times \dots \times p_n$ on aurait 2 divise $N - 6 p_1 \times p_2 \times \dots \times p_n$ c'est à dire 2 divise 1 ce qui est absurde. De même avec 3.

Finalement les seuls diviseurs premiers de N ne sont ni de la forme $6k + 5$, ni 2 et ni 3.

De fait chaque q_i est de la forme $6k + 1$ on en déduit que pour tout naturel $i \in \{1 ; 2 ; \dots ; m\}$ on a $q_i \equiv 1 [6]$ et donc $q_i^{\alpha_i} \equiv 1 [6]$ et par produit, on obtient la congruence $N \equiv 1 [6]$.

Concluons : On vient de montrer que si (H) est vraie alors on obtient $N \equiv 1 [6]$ mais aussi $N \equiv -1 [6]$, il y a là une contradiction. Finalement l'hypothèse selon laquelle il n'existe qu'un nombre fini de nombres premiers de la forme $6k + 5$ est donc fausse.

Exercice 98

Qui court deux lièvres à la fois n'en prend aucun.

Chiffrement affine mono-alphabétique

Le principe de ce chiffrement est le suivant :

→ On numérote les 26 lettres de l'alphabet de 0 (pour A) à 25 (pour Z) comme consigné dans le tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

→ On calcule les images de ces 26 entiers par une fonction affine $f: x \mapsto ax + b$ avec a et b deux entiers naturels et $a \neq 0$;

→ On prend les restes des images dans la division euclidienne par 26 ;

→ On remplace les lettres initiales par celles qui correspondent aux numéros donnés par les restes.

Le couple $(a; b)$ est la **clé secrète** du codage.

Si par exemple $a = 1$ et $b = 3$ alors le codage consiste à faire un décalage de la lettre de 3 crans (c'est le codage de Jules César : $A \rightarrow D; B \rightarrow E; \dots; X \rightarrow A; Y \rightarrow B; Z \rightarrow C$).

1. Démontrer que si a et 26 sont premiers entre eux, alors la clé $(a; b)$ est satisfaisante.

☞ Utiliser le théorème de GAUSS.

Dans les questions suivantes, on considère une clé $(a; b)$ telle que a et 26 sont premiers entre eux.

2. Montrer qu'il existe un entier relatif u tel que $a \times u \equiv 1 [26]$.

☞ Utiliser le théorème de BEZOUT.

3. Montrer que : Si $y \equiv ax + b [26]$, alors $x \equiv uy - bu [26]$

En déduire une fonction affine permettant de lire un message codé.

4. On considère la fonction de chiffrement f associée à la clé $(11; 8)$.

a. Coder ce proverbe chinois : « PARLER NE FAIT PAS CUIRE LE RIZ » (On ne compte pas les espaces et les accents).

b. Décoder le message : « IFA EAYIN ».

Corrigé

1. Il faut que deux lettres différentes ne reçoivent pas le même code. En effet, on a :

$ax + b \equiv ax' + b [26] \Leftrightarrow 26 | a(x' - x)$; si a et 26 sont premiers entre eux alors, d'après le théorème de Gauss, $26 | (x' - x)$; mais comme $-25 \leq x' - x \leq 25$ et que dans l'ensemble $\llbracket -25, 25 \rrbracket$ le seul multiple de 26 est 0, alors on déduit que $x' = x$ et par conséquent la clé $(a; b)$ est donc satisfaisante.

2. D'après le théorème de Bézout, il existe des entiers relatifs u et v tels que $au + 26v = 1$; alors $au \equiv 1 [26]$.

3. Si $y \equiv ax + b [26]$ alors $uy \equiv x + bu [26]$, car $au \equiv 1 [26]$; donc $x \equiv uy - bu [26]$.

La fonction $g : y \mapsto uy - bu$ convient pour décoder les messages.

4.a. La fonction de chiffrement est $f(x) = 11x + 8 [26]$. N'hésiter pas de compléter le tableau et de faire les calculs nécessaires (Le tout a été expliqué et il n'y a plus de secret)

Lettres Initiales	P	A	R	L	E	...	...	R	I	Z
Numéros	15	0	17	11	4	...	...	17	8	25
Numéros codés	17	8	13	25	0	...	...	13	18	23
Lettres codées	R	I	N	Z	A			N	S	X

b. Avec l'algorithme d'Euclide, on obtient $u = -7$. Donc $g(y) = -7y + 56$.

Lettres codées	I	F	A	E	A	Y	I	N
Numéros	8	5	0	4	0	24	8	13
Numéros décodés	0	21	4	2	4	18	0	17
Lettres décodées	A	V	E	C	E	S	A	R

Exercice 99

Il vaut mieux être le bec du coq que la queue du taureau.

Chiffrement de Hill ou chiffrement affine poly-alphabétique.

(Dans cet exercice, le chiffrement est par digramme c'est-à-dire par bloc de 2 lettres)

Partie A : Question de cours

Soit a, b, c, d des entiers relatifs et n un entier naturel non nul.

Montrer que si $a \equiv b [n]$ et $c \equiv d [n]$ alors $ac \equiv bd [n]$.

Partie B : Inverse de 23 modulo 26

On considère l'équation (E) : $23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1. Vérifier que le couple $(-9; -8)$ est solution de l'équation (E).

2. Résoudre alors l'équation (E).

3. En déduire un entier a tel que $0 \leq a \leq 25$ et $23a \equiv 1 [26]$.

Partie C : Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 : Chaque lettre du mot est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient un couple d'entiers $(x_1; x_2)$ où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 : $(x_1; x_2)$ est transformé en $(y_1; y_2)$ tel que : $(S_1) \begin{cases} y_1 \equiv 11x_1 + 3x_2 [26] \\ y_2 \equiv 7x_1 + 4x_2 [26] \end{cases}$ avec $\begin{cases} 0 \leq y_1 \leq 25 \\ 0 \leq y_2 \leq 25 \end{cases}$.

Étape 3 : $(y_1; y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance de l'étape 1.

Exemple : $\underbrace{TE}_{\text{mot en clair}} \rightarrow (19; 4) \rightarrow (13; 19) \rightarrow \underbrace{NT}_{\text{mot codé}}.$

1. Coder le mot ST.

2. On veut maintenant déterminer la procédure de décodage.

a. Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système (S_1) , vérifie les équations du système :

$$(S_2) \begin{cases} 23x_1 \equiv 4y_1 + 23y_2 [26] \\ 23x_2 \equiv 19y_1 + 11y_2 [26] \end{cases}$$

b. À l'aide de la partie B, montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système (S_2) ,

vérifie les équations du système $(S_3) : \begin{cases} x_1 \equiv 16y_1 + y_2 [26] \\ x_2 \equiv 11y_1 + 5y_2 [26] \end{cases}.$

c. Montrer que tout couple $(x_1; x_2)$ vérifiant les équations du système (S_3) , vérifie les équations du système (S_1) .

d. Décoder le mot YJ.

Corrigé

Partie A : Question de cours

Il s'agit de la compatibilité de la multiplication avec la congruence : n'hésiter pas de revoir le cours.

Partie B : Inverse de 23 modulo 26

1. On a : $23 \times (-9) - 26 \times (-8) = -207 + 208 = 1$. Donc le couple $(-9; -8)$ est solution de (E).

2. On a : $\begin{cases} 23x - 26y = 1 \\ 23 \times (-9) - 26 \times (-8) = 1 \end{cases}$ ce qui donne par différence membre à membre :

$$23 \times (x + 9) - 26 \times (y + 8) = 0 \text{ soit encore } 23 \times (x + 9) = 26 \times (y + 8) \quad (1).$$

Donc 23 divise $26(y + 8)$ et comme $23 \wedge 26 = 1$ alors selon Gauss 23 divise $y + 8$ c'est-à-dire qu'il existe un entier relatif k tel que $y + 8 = 23k$ et donc $y = -8 + 23k$.

En remplaçant, dans (1), $y + 8$ par $23k$, on obtient : $23(x + 9) = 26 \times 23k$ et donc : $x = -9 + 26k$.

Réciproquement, on vérifiera facilement que les couples $(-9 + 26k; -8 + 23k)$ sont solutions de (E).

Conclusion : $S_{(E)} = \{(-9 + 26k; -8 + 23k) / k \in \mathbb{Z}\}$.

3. Il s'agit de trouver un couple $(a; b)$ solution de (E) tel que sa première composante a vérifie $0 \leq a \leq 25$. Or, on sait qu'il existe un entier k tel que $a = -9 + 26k$. La condition sur a s'exprime donc par $0 \leq -9 + 26k \leq 25$. Il y a une seule valeur possible pour k : $k = 1$ et pour cette valeur, on a :

$$a = -9 + 26 = 17.$$

De l'égalité $23 \times 17 - 26b = 1$, on tire via le modulo 26 que $23 \times 17 \equiv 1 [26]$ car $26b \equiv 0 [26]$. Donc l'inverse de 23 modulo 26 est 17.

Partie C : Chiffrement de HILL

1. $\underbrace{ST}_{\text{mot en clair}} \xrightarrow{\text{Etape 1}} \underbrace{(18; 19)}_{(x_1; x_2)} \xrightarrow{\text{Etape 2}} \underbrace{(21; 20)}_{(y_1; y_2)} \xrightarrow{\text{Etape 3}} \underbrace{VU}_{\text{mot codé}}$

2. a. Soit $(x_1; x_2)$ une solution de (S_1) . Montrons que $(x_1; x_2)$ est solution de (S_2) .

On a : $\begin{cases} y_1 \equiv 11x_1 + 3x_2 [26] \times (-4) \\ y_2 \equiv 7x_1 + 4x_2 [26] \times 3 \end{cases} \Rightarrow \begin{cases} -44x_1 - 12x_2 \equiv -4y_1 [26] \\ 21x_1 + 12x_2 \equiv 3y_2 [26] \end{cases}$ et donc :

$$-23x_1 \equiv -4y_1 + 3y_2 [26].$$

De la même manière, on a : $\begin{cases} y_1 \equiv 11x_1 + 3x_2 [26] \times (-7) \\ y_2 \equiv 7x_1 + 4x_2 [26] \times 11 \end{cases} \Rightarrow \begin{cases} -77x_1 - 21x_2 \equiv -7y_1 [26] \\ 77x_1 + 44x_2 \equiv 11y_2 [26] \end{cases}$

Et toujours par somme, on obtient : $23x_2 \equiv -7y_1 + 11y_2 [26]$.

Or, d'une part, la relation $-23x_1 \equiv -4y_1 + 3y_2 [26]$ s'écrit :

$23x_1 \equiv 4y_1 - 3y_2 [26]$ ou encore $23x_1 \equiv 4y_1 + 23y_2 [26]$ car $-3 \equiv 23 [26]$. D'autre part, comme $-7 \equiv 19 [26]$ alors la relation $23x_2 \equiv -7y_1 + 11y_2 [26]$ s'écrit $23x_2 \equiv 19y_1 + 11y_2 [26]$.

D'où le système de congruences $\begin{cases} 23x_1 \equiv 4y_1 + 23y_2 [26] \\ 23x_2 \equiv 19y_1 + 11y_2 [26] \end{cases}$ CQFD.

b. On a déjà montré à la Partie B que $23 \times 17 \equiv 1 [26]$. Donc en multipliant chaque membre du système (S_2) par 17, on obtient :

$$\begin{cases} 23x_1 \times 17 \equiv 4y_1 \times 17 + 23y_2 \times 17 [26] \\ 23x_2 \times 17 \equiv 19y_1 \times 17 + 11y_2 \times 17 [26] \end{cases}$$

Soit : $\begin{cases} x_1 \equiv 68y_1 + y_2 [26] \\ x_2 \equiv 323y_1 + 187y_2 [26] \end{cases}$ et compte tenu des congruences : $68 \equiv 16 [26]$, $323 \equiv 11 [26]$ et

$187 \equiv 5 [26]$, on peut conclure que $(x_1; x_2)$ vérifie le système : $(S_3) \begin{cases} x_1 \equiv 16y_1 + y_2 [26] \\ x_2 \equiv 11y_1 + 5y_2 [26] \end{cases}$ CQFD.

c. Soit $(x_1; x_2)$ un couple vérifiant (S_3) . Montrons qu'il vérifie également le système (S_1) .

On a : $11x_1 + 3x_2 = 11(16y_1 + y_2) + 3(11y_1 + 5y_2) = 209y_1 + 26y_2$. Or $209 \equiv 1 [26]$ et $26 \equiv 0 [26]$, d'où :

$$11x_1 + 3x_2 \equiv y_1 [26].$$

De la même manière, on démontre que $7x_1 + 4x_2 \equiv y_2 [26]$.

D'où enfin $(x_1; x_2)$ vérifie bien le système (S_1) . Donc les systèmes (S_1) et (S_3) sont équivalents. Le système (S_1) sert à coder, le système (S_3) à décoder.

d. Le mot **YJ** correspond au couple $(y_1; y_2) = (24; 9)$. En appliquant les équations du système (S_3) qui

permettent le décodage, on obtient : $\begin{cases} x_1 \equiv 16 \times 24 + 9 [26] \\ x_2 \equiv 11 \times 24 + 5 \times 9 [26] \end{cases}$ ou encore $\begin{cases} x_1 \equiv 393 [26] \\ x_2 \equiv 309 [26] \end{cases}$

Or $393 \equiv 3 [26]$ et $309 \equiv 23 [26]$, d'où $(x_1; x_2) = (3; 23)$ et par suite la lecture du tableau de correspondance indique que le mot codé est **DX**.

Exercice 100

La bouche est la porte du malheur.

Le chiffrement affine mono-alphabétique (voir exercice n°98) est trop facile à « craquer » sur le plan mathématique. C'est pourquoi le diplomate français **Blaise de Vigenère** eut l'idée d'utiliser une clé pour doper le chiffrement affine. Cette clé peut être un mot, une phrase, un paragraphe ou même carrément un livre !!! Si l'on veut coder la phrase « il fait beau et chaud » avec la clé « beau ciel », on procède de la façon suivante :

Etape 1 : On superpose la phrase et la clé (que l'on répète autant de fois qu'il le faut) :

I	L	F	A	I	T	B	E	A	U	E	T	C	H	A	U	D
B	L	E	U	C	I	E	L	B	L	E	U	C	I	E	L	B

Etape 2 : On associe à une lettre de la phrase son entier x_i , et à la lettre correspondante de la clé son entier y_i .

Etape 3 : On détermine z_i tel que $\begin{cases} x_i + y_i \equiv z_i [26] \\ 0 \leq z_i \leq 25 \end{cases}$.

Etape 4 : On associe à l'entier z_i sa lettre.

1. Coder la phrase « il fait beau et chaud » avec la clé « beau ciel ».

2. Quel est le gros intérêt de ce chiffrement par rapport au chiffrement affine.

3. On s'intéresse maintenant à la procédure de décodage.

a. Montrer que cette procédure est élémentaire lorsque l'on connaît la clé.

b. Décoder la phrase suivante : « DZQGGBIDZPYR ».

Corrigé

1. Pour répondre facilement à la question, il vaut mieux faire un tableau :

	I	L	F	A	I	T	B	E
	B	L	E	U	C	I	E	L
x_i	8	11	5	0	8	19	1	4
y_i	1	11	4	20	2	8	4	11
$x_i + y_i$	9	22	9	20	10	27	5	15
z_i	9	22	9	20	10	27	5	15
	J	W	J	U	K	B	F	P

	A	U	E	T	C	H	A	U	D
	B	L	E	U	C	I	E	L	B
x_i	0	20	4	19	2	7	0	20	3
y_i	1	11	4	20	2	8	4	11	1
$x_i + y_i$	1	31	8	39	4	15	4	31	4
z_i	1	31	8	39	4	15	4	31	4
	B	F	I	N	E	P	E	F	E

Finalement, la phrase codée est « JWJUKBFPBFINEPEFE ».

2. Le gros intérêt est qu'une même lettre n'est pas toujours codée par la même lettre, tout dépend de la clé...

3.a. Comme $x_i + y_i = z_i$ [26], quand on connaît la clé, comme y_i est également connu, il suffit de trouver x_i tel que : $\begin{cases} x_i = z_i - y_i \text{ [26]} \\ 0 \leq x_i \leq 25 \end{cases}$.

b. Pour décoder la phrase, on fait le tableau suivant en appliquant la question précédente pour trouver la valeur de x .

	D	Z	Q	G	G
	B	L	E	U	C
z_i	3	25	16	6	6
y_i	1	11	4	20	2
$z_i - y_i$	2	14	12	-14	4
x_i	2	14	12	12	4
	C	O	M	M	E

	B	I	D	Z	P	Y	R
	I	E	L	B	L	E	U
z_i	1	8	3	25	15	24	17
y_i	8	4	11	1	11	4	20
$z_i - y_i$	-7	4	-8	24	4	20	-3
x_i	19	4	18	24	4	20	23
	T	E	S	Y	E	U	X

La phrase est « comme tes yeux ».

Exercice 101

C'est une belle harmonie quand le faire et le dire vont ensemble.

Chiffrement par exponentiation

Partie A : On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. Vérifier que le couple (13, 3) est solution de cette équation.

2. Déterminer l'ensemble des couples de relatifs solutions de l'équation (E).

Partie B : Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation : $25g - 108c = 1$.

On rappelle le petit théorème de Fermat : si p est un nombre premier et a un entier non divisible par p alors a^{p-1} est congru à 1 modulo p , ce que l'on note $a^{p-1} \equiv 1 [p]$.

1. Soit x un entier naturel. Démontrer que si $x \equiv a [7]$ et $x \equiv a [19]$ alors $x \equiv a [133]$.

2. a. On suppose que a n'est pas un multiple de 7.

Démontrer que $a^6 \equiv 1 [7]$ puis que $a^{108} \equiv 1 [7]$. En déduire que $(a^{25})^g \equiv a [7]$.

b. On suppose que a est un multiple de 7. Démontrer que $(a^{25})^g \equiv a [7]$.

c. On admet que pour tout entier naturel a , $(a^{25})^g \equiv a [19]$. Démontrer que $(a^{25})^g \equiv a [133]$.

Partie C : On note A l'ensemble des entiers naturels a tels que : $1 \leq a \leq 26$.

Un message, constitué d'entiers appartenant à A , est codé puis décodé. La phase de codage consiste à associer à chaque entier a de A , l'entier r tel que $a^{25} \equiv r [133]$ avec $0 \leq r < 133$.

La phase de décodage consiste à associer à r , l'entier r_1 tel que $r^{13} \equiv r_1 [133]$ avec $0 \leq r_1 < 133$.

1. Justifier que $r_1 \equiv a [133]$.

2. Un message codé conduit à la suite des 2 entiers suivants : 128 et 59. Décoder ce message.

Corrigé

Partie A : On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. $25 \times 13 - 108 \times 3 = 325 - 324 = 1$, le couple $(13 ; 3)$ est bien solution de l'équation (E).

2. Le couple $(13 ; 3)$ est une solution particulière de (E) c'est-à-dire que : $25 \times 13 - 108 \times 3 = 1$.

$(x ; y)$ est solution de (E) équivaut à $25x - 108y = 1$. Par différence des deux identités, on trouve :

$$25(x - 13) = 108(y - 3) \quad (1)$$

Comme 108 et 25 sont premiers entre eux et $25 \mid 108(y - 3)$ alors $25 \mid y - 3$ c'est-à-dire qu'il existe un entier relatif k tel que : $y - 3 = 25k$ ou encore $y = 3 + 25k$. En remplaçant $y - 3$ par $25k$ dans (1), on trouve $x = 13 + 108k$. Donc l'ensemble des couples d'entiers relatifs solutions de l'équation (E) est :

$$\{(13 + 108k ; 3 + 25k) / k \in \mathbb{Z}\}.$$

Partie B : Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation : $25g - 108c = 1$.

1. Soit x un entier naturel.

Si $x \equiv a [7]$ alors 7 divise $x - a$. De même $x \equiv a [19]$ implique que 19 divise $x - a$. Or $7 \wedge 19 = 1$ donc $7 \times 19 = 133$ divise $x - a$. Ce résultat peut être écrit $x \equiv a [133]$.

2.a. $\left. \begin{array}{l} 7 \text{ est un nombre premier} \\ a \text{ n'est pas un multiple de } 7 \end{array} \right\} \Rightarrow a^{7-1} \equiv 1 [7]$ selon le petit théorème de Fermat. Donc $a^6 \equiv 1 [7]$.

D'autre part, $a^{108} = a^{6 \times 18} = (a^6)^{18} \equiv 1^{18} [7] \equiv 1 [7]$, d'où :

$$(a^{25})^g = a^{25g} = a^{1+108c} = a \times (a^{108})^c \equiv a \times 1^c \equiv a [7].$$

Donc, si a n'est pas un multiple de 7 alors : $a^6 \equiv 1 [7]$, $a^{108} \equiv 1 [7]$ et $(a^{25})^g \equiv a [7]$.

b. Si a est un multiple de 7 alors $a \equiv 0 [7]$ et par suite : $(a^{25})^g = a^{25g} \equiv 0 \equiv a [7]$.

Donc, si a est un multiple de 7 alors $(a^{25})^g \equiv a [7]$.

c. On admet que pour tout entier naturel a , $(a^{25})^g \equiv a [19]$.

On a : $\left\{ \begin{array}{l} (a^{25})^g \equiv a [7] \text{ (démontré en B. 2.)} \\ (a^{25})^g \equiv a [19] \text{ (admis en B. 2. c.)} \end{array} \right.$ donc en appliquant les résultants du B.1. pour $x = (a^{25})^g$,

on peut conclure que pour tout entier naturel a : $(a^{25})^g \equiv a [133]$.

Partie C

1. On sait déjà que le couple $(g ; c) = (13 ; 3)$ vérifie l'équation (E) c'est-à-dire que : $25g - 108c = 1$ (Partie A).

On peut donc appliquer les résultats de la question 2.c. de la partie B : $r_1 \equiv r^{13} \equiv (a^{25})^{13} \equiv a [133]$.

2. On a : $128 \equiv -5 [133]$, donc $128^{13} \equiv (-5)^{13} \equiv -131 \equiv 2 [133]$ et aussi :

$$59^{13} \equiv (59^4)^3 \times 59 \equiv (-3)^3 \times 59 \equiv 3 [133].$$

Donc le message avant codage était les deux entiers suivants : **2 3**.

Exercice 102

Le courage est l'art de dissimuler sa peur.

Le système cryptographique RSA - 1^{er} Épisode

Les chiffrements affines, de Vigenère et de Hill et les méthodes de plus en plus sophistiquées qui leur succédèrent jusqu'à la fin des années 1970 ont toutes posé un problème important : celui de l'échange des clés entre l'émetteur et le destinataire du message, la clé utilisée étant la même pour le chiffrement que pour le déchiffrement (on parle de clé « symétrique »). En 1975, trois américains (Diffie, Hellman

et Merkle) ont eu l'idée d'utiliser une clé « asymétrique » : la clé de chiffrement (clé publique) serait différente de la clé de déchiffrement (clé privée).



Ron Rivest, Adi Shamir et Léonard Adleman

Il restait à concrétiser cette idée en trouvant une fonction de chiffrement adaptée.

Trois autres américains Ron Rivest, Adi Shamir et Léonard Adleman (photo ci-contre) ont concrétisé les travaux de D.H.M, et donné naissance au système R.S.A en 1978.

Le RSA est basé sur la théorie des nombres premiers, et sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition « rapide », surtout d'un très grand nombre en facteurs premiers. L'usage du R.S.A ne s'est généralisé qu'à la fin des années 1990 avec l'arrivée d'Internet et il est utilisé actuellement dans plus de 85% des échanges sécurisés mondiaux.

Partie I

1. Propriété fondamentale

$n = p q$ est le produit de deux nombres premiers p et q distincts. On pose $m = (p - 1)(q - 1)$ et on note c un nombre premier avec m . On note x un entier naturel.

a. Démontrer qu'il existe des entiers d et k tels que : $c d = k m + 1$ (c'est à dire $c d \equiv 1$ modulo m)

b. Cas où x est non divisible par p .

Démontrer que $x^{p-1} \equiv 1$ modulo p

En déduire que $x^{km} \equiv 1$ modulo p puis que $x^{cd} \equiv x$ modulo p .

Cas où x est divisible par p .

Démontrer que $x^{cd} \equiv x$ modulo p .

c. Démontrer de façon analogue que pour tout x entier naturel, on a : $x^{cd} \equiv x$ modulo q .

d. En déduire que pour tout entier naturel x , $x^{cd} \equiv x$ modulo n .

$n = p q$ (n étant un entier naturel, p et q étant premiers).

La connaissance de n permet de trouver les entiers m , c , et d de la partie 1 et les messages à crypter sont des entiers x compris entre 0 et $n - 1$.

Cryptage : x est crypté par $C(x)$ congru x^c modulo n . Les données n et a sont nécessaires pour crypter et le couple $(n ; c)$ est la clé publique, connue de tous.

Décryptage : y est décrypté par $D(y)$ congru y^d modulo n .

Les données n et b sont nécessaires pour décrypter et d est la clé privée, connue seulement de la personne qui reçoit le message. On peut vérifier que $D(C(x))$ congru $(x^c)^d$ congru x^{cd} congru x modulo n ; on retrouve donc la valeur x après cryptage, puis décryptage.

Partie II

1. Mariem souhaite recevoir en message crypté l'âge de Coumba. elle choisit les entiers $p = 3$ et $q = 11$.

a. Calculer n et m , puis déterminer le plus petit entier qu'elle peut choisir comme valeur pour c .

b. Déterminer alors le plus petit entier qu'elle peut choisir pour d .

c. Mariem envoie sa clé publique $(33 ; 3)$ à Coumba. Cette dernière crypte son âge et lui envoie le nombre 29. Retrouver l'âge de Coumba.

2. En retour, Coumba souhaite que Mariem lui envoie en message crypté son numéro de téléphone. Les numéros sont cryptés deux par deux.

a. justifier que n doit être supérieur ou égal à 100.

b. Montrer que la clé publique la plus petite possible que Coumba peut envoyer est alors $(106 ; 3)$.

c. Crypter alors avec cette clé le numéro de téléphone de Mariem : 06 13 87 11 45.

Corrigé

Partie I

1. a. c est un nombre premier avec m donc d'après le théorème de Bézout, il existe deux nombres entiers relatifs u et v tels que $c u + m v = 1$ donc $c u = -m v + 1$ en posant $d = u$ et $-v = k$; il existe des entiers d et k tels que : $cd = km + 1$.

b. Cas où x est non divisible par p .

p est un nombre premier et x est non divisible par p donc x est premier avec p donc d'après le petit théorème de Fermat, $x^{p-1} \equiv 1 [p]$.

$x^{p-1} \equiv 1 [p]$ donc $(x^{p-1})^{q-1} \equiv 1^{q-1} [p]$ soit $x^m \equiv 1 [p]$ et donc $(x^m)^k \equiv 1^k [p]$ soit $x^{km} \equiv 1 [p]$ et donc : $x^{cd} = x^{km+1} = x^{km} \times x$ or $x^{km} \equiv 1 [p]$ donc $x^{cd} \equiv x [p]$.

c. Si x est divisible par q , alors $x \equiv 0 [q]$ donc $x^{cd} \equiv 0 [q]$ donc $x^{cd} \equiv x [q]$.

Si x est non divisible par q , alors q est un nombre premier et x est non divisible par q donc x est premier avec q donc d'après le petit théorème de Fermat, $x^{q-1} \equiv 1 [q]$.

$x^{q-1} \equiv 1 [q]$ donc $(x^{q-1})^{p-1} \equiv 1^{p-1} [q]$ soit $x^m \equiv 1 [q]$ donc $(x^m)^k \equiv 1^k [q]$ soit $x^{km} \equiv 1 [q]$.

$x^{cd} = x^{km+1} = x^{km} \times x$ or $x^{km} \equiv 1 [q]$ donc $x^{cd} \equiv x [q]$. Dans tous les cas : $x^{cd} \equiv x [q]$.

d. p et q divisent $x^{cd} - x$, p et q sont deux entiers naturels premiers donc premiers entre eux donc, d'après le théorème de Gauss, pq divise $x^{cd} - x$. Pour tout entier naturel x , $x^{cd} \equiv x [n]$.

Partie II

1. Mariem souhaite recevoir en message crypté l'âge de Coumba. Elle choisit $p = 3$ et $q = 11$.

a. Calculer n et m , puis déterminer le plus petit entier qu'il peut choisir pour c .

$$n = pq = 3 \times 11 = 33$$

$$m = (p-1)(q-1) = 2 \times 10 = 20 = 2^2 \times 5$$

c est un nombre premier avec m donc le plus petit entier possible pour c est 3.

b. Il faut résoudre : $cu + mv = 1$ avec $c = 3$ et $m = 20$ soit $3u + 20v = 1$, une solution est $u = 7$ et

$v = -1$. On a : $\begin{cases} 3u + 20v = 1 \\ 3 \times 7 + 20 \times (-1) = 1 \end{cases}$ donc par différence terme à terme : $3(u-7) + 20(v+1) = 0$ soit : $3(u-7) = -20(v+1)$.

3 et 20 sont premiers entre eux et 20 divise $3(u-7)$ donc d'après le théorème de Gauss, 20 divise $u-7$ donc il existe un entier relatif k tel que $u-7 = 20k$ donc $u = 20k + 7$.

$d = u$ donc $d = 20k + 7$, le plus petit entier naturel qu'il peut choisir pour d est 7.

c. Le couple $(n; c)$ est la clé publique donc $n=33$ et $c=3$.

Décryptage : y est décrypté par $D(y)$ congru y^d modulo n .

$$D(y) \equiv 29^7 \text{ modulo } 33$$

$$29 \equiv -4 \text{ modulo } 33$$

$$29^2 \equiv 16 \text{ modulo } 33$$

$$29^3 \equiv -64 \text{ modulo } 33 \text{ donc } 29^3 \equiv 2 \text{ modulo } 33$$

$$29^6 \equiv 2^2 \text{ modulo } 33$$

$$29^7 \equiv 4 \times 29 [33] \Leftrightarrow 29^7 \equiv 4 \times (-4) [33] \Leftrightarrow 29^7 \equiv 17 [33]$$

29 est décrypté par 17. Coumba a 17 ans.

2. a. Justifier que n doit être supérieur ou égal à 100

Le nombre x à crypter est au maximum égal à 99 or $0 \leq x \leq n-1$ donc $n \geq 100$.

b. La plus petite valeur possible de c est 3 d'après la question 1. a.

$n = pq$ est le produit de deux nombres premiers p et q distincts.

Le plus petit nombre premier possible est $p = 2$, or $n = pq$ et $n \geq 100$ donc $2q \geq 100$ donc $q \geq 50$

Le plus petit nombre premier supérieur à 50 est 53 donc $q = 53$ et $n = 2 \times 53 = 106$

La clé publique la plus petite possible que Coumba peut envoyer est alors le couple $(106; 3)$.

c.

x	06	13	87	11	45
x^3	216	2197	658503	1331	91125
Quotient de x^3	2	20	6212	12	859
Reste de x^3	4	77	31	59	71

Le numéro de téléphone de Mariem : 06 13 87 11 45 est codé par : 04 77 31 59 71.

Exercice 103

La même gourde qui a contenu du piment, peut vide, faire éternuer.

Le système cryptographique RSA - 2^e Épisode

Protocole RSA pour envoyer un message crypté : Une personne nommée « l'Émetteur » veut transmettre une information secrète à une autre personne dite « le Destinataire ».

(a) Création des clefs.

Destinataire construit un quadruplet de nombres (p, q, e, d) tel que p et q sont deux nombres premiers; on pose $n = pq$, e est un entier premier avec le produit $(p - 1)(q - 1)$; d est un entier positif tel que $ed - 1$ est un multiple de $(p - 1)(q - 1)$, c'est-à-dire tel que $ed \equiv 1 \pmod{(p - 1)(q - 1)}$.

On sait alors d'après l'énoncé du théorème du RSA que, si A est un entier quelconque, alors $A^{ed} \equiv A \pmod{n}$, et c'est cette identité qui va tout faire fonctionner.

Le nombre d constitue la clef secrète de Destinataire.

(b) Destinataire rend publics n et e , qui constituent la clé publique. Il ne publie surtout pas p , q ou d . Le nombre d constitue la clé secrète du destinataire.

(c) Émetteur, qui veut transmettre une information secrète à Destinataire, transforme son information en un nombre entier A , inférieur à n (ou en plusieurs si nécessaire), en utilisant des conventions connues de tous (provenant, par exemple, des codes numériques des caractères typographiques, ou en prenant $a = 01$, $b = 02$, etc.).

(d) Émetteur calcule, $B \equiv A^e \pmod{n}$, envoie B à Destinataire par un canal qui n'a pas besoin d'être protégé (par exemple, le courrier électronique).

(e) Destinataire, pour décoder B , calcule $B^d \pmod{n}$, ce qui lui redonne A , car, d'après le théor. du RSA, on a :

$$B^d \equiv A^{ed} \equiv A \pmod{n}.$$

Théorème du RSA :

Soient p et q deux nombres premiers distincts.

On pose $n = p \cdot q$ et $m = (p - 1)(q - 1)$.

Si e est un nombre premier avec m alors :

(1) il existe un entier $d > 0$ tel que $ed \equiv 1 \pmod{m}$

(2) pour cet entier d et pour tout entier a , on a : $a^{ed} \equiv a \pmod{n}$

Partie théorique :

1. Montrer que si la condition « e et m premiers entre eux » n'est pas remplie, il n'est pas possible de trouver un tel entier d .

2. a. Montrer que si p et q sont deux nombres premiers, alors : $\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases} \Leftrightarrow a \equiv b \pmod{pq}$.

Cette équivalence est-elle encore vraie lorsque p ou q n'est pas premier ?

b. Montrer que dans le théorème du RSA, il existe un entier r tel que : $ed = (p - 1)r + 1$.

En déduire que $a^{ed} \equiv a \pmod{p}$.

c. Montrer de même que $a^{ed} \equiv a \pmod{q}$ et conclure.

Partie Pratique : Le couple $(n; e)$ est la clef publique et le nombre d est la clef cachée.

On intercepte avec la clef publique $(8633; 1225)$ le message : 736 ; 8523 ; 916 ; 6630 ; 279.

Comme le nombre 8633 n'est pas très gros, on peut facilement, à l'aide d'un programme, trouver la clef secrète et décoder le message. Que dit ce message?

Corrigé

Partie théorique :

1. Soit $m = 6$ et $e = 4$, s'il existe un entier $d > 0$ tel que $ed \equiv 1 \pmod{m}$ alors on a :

$4d \equiv 1 \pmod{6}$ donc il existe un entier relatif q tel que $4d = 6q + 1$. Or $4d$ est un nombre pair, $6q + 1$ est un nombre impair donc $4d \neq 6q + 1$. La propriété (1) n'est pas valide si e et m ne sont pas premiers entre eux.

2. a. Si $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$ alors p divise $a - b$ et q divise $a - b$, p et q sont deux nombres premiers distincts donc sont premiers entre eux donc d'après le théorème de Gauss, pq divise $a - b$ donc :

$$a \equiv b \pmod{pq}.$$

Réciproquement : si $a \equiv b \pmod{pq}$, il existe un entier relatif n tel que $a - b = npq$.

nq est un entier relatif donc p divise $a - b$ donc $a \equiv b \pmod{p}$

np est un entier relatif donc q divise $a - b$ donc $a \equiv b \pmod{q}$

donc si $a \equiv b \pmod{pq}$ alors $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$ d'où l'équivalence : $\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases} \Leftrightarrow a \equiv b \pmod{pq}$.

Soit $p = 3$ et $q = 6$:

Soit $a = 6$, $b = 12$ alors $a - b = 6$ donc $a \equiv b \pmod{3}$ et $a \equiv b \pmod{6}$

$a - b = 6$ et $pq = 18$ donc $pq > a - b$ donc pq ne divise pas $a - b$, et donc on n'a pas $a \equiv b \pmod{pq}$.

La propriété ne s'applique pas si p ou q n'est pas premier.

b. Dans le théorème du RSA, $ed \equiv 1 [m]$ donc il existe un entier k tel que : $ed = (p-1)(q-1)k + 1$

Soit $r = (q-1)k$ alors r est un entier et $ed = (p-1)r + 1$ et $a^{ed} = a^{(p-1)r+1} = a^{(p-1)r} \times a$.

si a n'est pas divisible par p , p est un nombre premier donc, d'après le petit théorème de Fermat : $a^{p-1} \equiv 1 [p]$ donc $a^{(p-1)r} \equiv 1 [p]$ et par suite $a^{(p-1)r} \times a \equiv a [p]$ soit $a^{ed} \equiv a [p]$.

Si a est divisible par p , alors $a \equiv 0 [p]$ donc $a^{ed} \equiv 0 [p]$ donc $a^{ed} \equiv a [p]$.

Donc dans tous les cas $a^{ed} \equiv a [p]$.

c. Dans le théorème du RSA, $ed \equiv 1 [m]$ donc il existe un entier k tel que : $ed = (p-1)(q-1)k + 1$.

Soit $r' = (q-1)k$ alors r' est un entier et $ed = (q-1)r' + 1$ et donc : $a^{ed} = a^{(q-1)r'+1} = a^{(q-1)r'} \times a$.

si a n'est pas divisible par q , q est un nombre premier donc, d'après le petit théorème de Fermat : $a^{q-1} \equiv 1 [q]$ donc $a^{(q-1)r'} \equiv 1 [q]$ et par suite $a^{(q-1)r'} \times a \equiv a [q]$ soit $a^{ed} \equiv a [q]$.

Si a est divisible par q , alors $a \equiv 0 [q]$ donc $a^{ed} \equiv 0 [q]$ donc $a^{ed} \equiv a [q]$.

Donc dans tous les cas $a^{ed} \equiv a [q]$.

On a : $a^{ed} \equiv a [p]$ et $a^{ed} \equiv a [q]$

p et q sont deux nombres premiers distincts donc d'après la propriété démontrée à la question 2.a, $a^{ed} \equiv a [pq]$ soit $a^{ed} \equiv a [n]$.

Partie Pratique :

$n = 8633$ et $e = 1225$, déterminons s'il existe p et q deux nombres premiers tels que :

$$n = pq \text{ et } m = (p-1)(q-1).$$

$8633 = 89 \times 97$, les entiers 89 et 97 sont deux nombres premiers donc :

$$m = 88 \times 96 = 28 \times 3 \times 11 = 8448$$

$$e = 52 \times 72$$

donc e est un nombre premier avec m : $ed \equiv 1 [m] \Leftrightarrow 1225 \times d \equiv 1 [8448]$ donc $d = 3193$.

Exercice 104

Les bonnes idées n'ont pas d'âge, elles ont seulement de l'avenir.

Nombres de Mersenne et test de Lucas-Lehmer

Partie A : Le but de cette partie est de démontrer que l'ensemble des nombres premiers est infini en raisonnant par l'absurde.

1. On suppose qu'il existe un nombre fini de nombres premiers que l'on notera : $p_1, p_2, \dots, p_n$.

On considère le nombre E égal au produit de tous les nombres premiers augmenté de 1 :

$$E = p_1 \times p_2 \times \dots \times p_n + 1$$

Démontrer que E est un entier supérieur ou égal à 2, et que E est premier avec chacun des entiers $p_1, p_2, \dots, p_n$.

2. En utilisant le fait que E admet un diviseur premier conclure.

Partie B

Pour tout entier naturel $k > 2$, on pose $M_k = 2^k - 1$. On dit que l'entier M_k est le k -ième nombre de Mersenne.

1. a. Reproduire et compléter le tableau suivant, qui donne quelques valeurs de M_k :

k	2	3	4	5	6	7	8	9	10
M_k	3								

b. D'après le tableau précédent, si k est un nombre premier, peut-on conjecturer que le nombre M_k est premier ?

2. Soient p et q deux entiers naturels non nuls.

a. Justifier l'égalité : $1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1} = \frac{2^{pq}-1}{2^p-1}$.

b. En déduire que $2^{pq} - 1$ est divisible par $2^p - 1$.

c. En déduire que si un entier k supérieur ou égal à 2 n'est pas premier, alors M_k ne l'est pas non plus.

3. a. Prouver que le nombre de Mersenne M_{11} n'est pas premier.

b. Que peut-on en déduire concernant la conjecture de la question 1. b. ?

Partie C : Le test de Lucas-Lehmer permet de déterminer si un nombre de Mersenne donné est premier.

Ce test utilise la suite numérique (u_n) définie par $u_0 = 4$ et pour tout entier n : $u_{n+1} = u_n^2 - 2$.

Si n est un entier naturel supérieur ou égal à 2, le test permet d'affirmer que le nombre M_n est premier si et seulement si $u_{n-2} \equiv 0 \text{ modulo } M_n$. Cette propriété est admise dans la suite.

1. Utiliser le test de Lucas-Lehmer pour vérifier que le nombre de Mersenne M_5 est premier.

2. Soit n un entier naturel supérieur ou égal à 3.

L'algorithme suivant, qui est incomplet, doit permettre de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer.

<i>Variables</i>	<i>u, M, n et i sont des entiers naturels</i>
<i>Initialisation</i>	<i>u prend la valeur 4 Demander un entier $n > 3$</i>
<i>Traitement</i>	<i>M prend la valeur Pour i allant de 1 à ... faire u prend la valeur ... Fin Pour Si M divise u alors afficher «M.....» » sinon afficher «M.....»</i>

Recopier et compléter cet algorithme de façon à ce qu'il remplisse la condition voulue.

Corrigé

Partie A : Il s'agit de la démonstration d'Euclide de l'infinitude des nombres premiers qui date d'il y a 23 siècles !

1. On suppose qu'il existe un nombre **fini** de nombres premiers notés $p_1, p_2, \dots, p_n$. On considère le nombre défini par $E = p_1 \times p_2 \times \dots \times p_n + 1$. Le nombre 2 est premier donc il est dans la liste $\{p_1, p_2, \dots, p_n\}$; donc le produit de ces nombres p_i est supérieur ou égal à 2 et par conséquent E est supérieur strictement à 3.

L'écriture $E = p_1 \times p_2 \times \dots \times p_n + 1$ traduit le fait que le reste dans la division euclidienne de E par chacun des p_i est égal à 1. Donc E est premier avec chacun des p_i .

2. On sait que tout entier supérieur à 2 admet au moins un diviseur premier. Cela s'applique clairement à E . Donc E admet au moins un diviseur premier d . Ce diviseur ne peut être égal à aucun des p_i . D'où l'existence d'un autre nombre premier qui n'est ni p_1 , ni p_2 , ni ..., ni p_n , ce qui contredit de toute évidence l'hypothèse faite au départ. Il existe donc une infinité de nombres premiers.

Partie B : Pour tout entier $k > 2$, on pose $M_k = 2^k - 1$. On dit que M_k est le k -ième nombre de Mersenne.

1.a. On calcule M_k pour quelques valeurs de k :

k	2	3	4	5	6
M_k	3 premier	7 premier	$15 = 3 \times 5$	31 premier	$63 = 7 \times 9$
k	7	8	9	10	
M_k	127 premier	$255 = 5 \times 51$	$511 = 7 \times 73$	$1023 = 3 \times 341$	

b. D'après le tableau, on peut conjecturer que si k est premier alors M_k est premier.

2. Soient p et q deux entiers naturels non nuls.

a. On a : $1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1}$ est la somme de q termes consécutifs de la suite géométrique de 1^{er} terme 1 et de raison 2^p ; D'où :

$$1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1} = 1^{\text{er}} \text{ terme} \times \frac{1 - \text{raison}^{\text{nombre de termes}}}{1 - \text{raison}} = \frac{(2^p)^q - 1}{2^p - 1}.$$

b. Le nombre $1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1}$ est entier et, d'après l'égalité précédente, on a :

$(1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1}) \times (2^p - 1) = 2^{pq} - 1$; d'où $2^{pq} - 1$ est divisible par $2^p - 1$.

c. Soit k un nombre non premier ; alors il existe deux entiers naturels p et q tels que : $p \geq 2, q \geq 2$ et $k = p \times q$. On a donc $M_k = 2^k - 1 = 2^{pq} - 1$ est divisible par $2^p - 1$ d'après la question précédente. Comme $p \geq 2$ alors $2^p - 1 \geq 3$ et donc M_k n'est pas premier.

Remarque : On vient de démontrer que :

Si k est composé alors M_k est composé (Forme logique : $P \Rightarrow Q$).

On peut donc déduire que sa contraposée, qui lui est équivalente, est vraie :

Si M_k est premier alors k est premier (Forme logique : $\text{non}Q \Rightarrow \text{non}P$).

Cette dernière implication peut constituer un test de primalité mais qui n'est pas du tout pratique car on a l'inégalité $M_k \geq k$.

3.a. $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ et donc M_{11} n'est pas premier.

b. La conjecture de la question 1.b. est donc fautive : 11 est premier et M_{11} n'est pas premier.

Partie C : Soit (u_n) la suite définie sur $\mathbb{N}$ par : $\begin{cases} u_0 = 4 \\ u_{n+1} = u_n^2 - 2 \end{cases}$ pour tout naturel n .

1. D'après le test de Lucas-Lehmer, M_5 est premier si et seulement si $u_3 \equiv 0 \pmod{M_5}$.

On a : $M_5 = 2^5 - 1 = 31$; $u_0 = 4$; $u_1 = u_0^2 - 2 = 14$;

$u_2 = u_1^2 - 2 = 194$; $u_3 = u_2^2 - 2 = 37\,634 = 31 \times 1\,214$.

Donc u_3 est divisible par M_5 et le test de Lucas-Lehmer est vérifié pour $k = 5$.

2. L'algorithme suivant permet de vérifier si le nombre de Mersenne M_n est premier, en utilisant le test de Lucas-Lehmer :

Variables	u, M, n et i sont des entiers naturels
Initialisation	u prend la valeur 4 Demander un entier $n > 3$
Traitement	M prend la valeur $\ll 2^n - 1 \gg$ Pour i allant de 1 à $\ll n - 2 \gg$ faire u prend la valeur $\ll u^2 - 2 \gg$ Fin Pour Si M divise u alors afficher $\ll M$ est premier $\gg$ sinon afficher $\ll M$ n'est pas premier $\gg$

Exercice 105	Si Dieu exauçait la prière des chiens, il ferait pleuvoir des os.
---------------------	--

Le plus grand nombre premier connu à ce jour est $2^{57885161} - 1$: c'est un nombre de Mersenne, le 47^{ème} nombre premier connu de cette catégorie. Il a été découvert le 25 janvier 2013 par trois professeurs Curtis Cooper, G. Woltman, S. Kurowski exerçant à University of Central Missouri dans le cadre du projet GIMPS (Internet Mersenne Prime Search). Ce nombre est composé de plus de 17 millions de chiffres et remplirait près de 20 livres de 500 pages environ soit un fichier de 22 Mo !! La vérification de sa primalité a nécessité 39 jours de calcul continu sur des puissants ordinateurs !!! Quels sont ses deux derniers chiffres ?

Remarque : Aujourd'hui le plus grand nombre premier connu est un nombre de Mersenne, ce n'est plus le 47^{ème} mais plutôt le 49^{ème}, $2^{74\,207\,281} - 1$, qui comprend 22 338 618 chiffres et qui a été découvert le 7 janvier 2016 (Cet exercice étant rédigé en septembre 2015, j'ai été rattrapé par cette nouvelle découverte. Donc j'ai laissé l'énoncé intact mais je recommande vivement au lecteur de reprendre l'exercice avec ce nouveau record).

Corrigé

Il s'agit donc de calculer $p = 2^{57885161} - 1$ modulo 100. Puisque $100 = 2^2 \times 5^2 = 4 \times 25$, le théorème chinois nous invite à calculer ce nombre modulo 4 et 25, pour en déduire sa valeur modulo 100.

Tout d'abord, modulo 4, l'énorme puissance de 2 se réduit évidemment à 0. On a donc $p \equiv -1 \pmod{4}$.

Ensuite, il faut examiner le comportement des puissances de 2 modulo 25. Pour cela, on peut par exemple remarquer que $2^{10} = 1024 \equiv 24 \equiv -1 \pmod{25}$. En élevant au carré, on a donc $2^{20} \equiv 1 \pmod{25}$. Par ailleurs, il est visible que $57885161 \equiv 1 \pmod{20}$. On peut donc trouver un entier $r \in \mathbb{N}$ (qu'il serait facile mais inutile de calculer) tel que l'on ait $57885161 = 20r + 1$. On peut alors calculer la réduction de p modulo 25 :

$$p = 2^{20r+1} - 1 = 2 \times (2^{20})^r - 1 \equiv 2 \times 1^r - 1 \equiv 1 \pmod{25}.$$

Ainsi, $p \equiv -1 \pmod{4}$ et $p \equiv 1 \pmod{25}$. Le théorème chinois assure que cela détermine la réduction de p modulo 100. Ici, c'est assez facile à vérifier à la main : si un nombre est congru à 1 modulo 25, il est congru à 1, 26, 51 ou 76 modulo 100. De toutes ces possibilités, seule la troisième est congrue à -1 modulo 4.

On en déduit donc $p \equiv 51 \pmod{100}$ et les deux derniers chiffres du plus grand nombre premier connu à ce jour sont 5 et 1.

Exercice 106

Le professeur est comme une barque qui attend les passagers pour leur faire traverser le fleuve.

Soit n un entier naturel non nul et $\sigma(n)$ la somme des chiffres de n en base 10.

Partie A

- Justifier qu'il existe un naturel p tel que : $10^p \leq n < 10^{p+1}$. Quel est le nombre de chiffres de n ?
- Montrer que $p = E(\log_{10}(n))$ où $E(x)$ représente la partie entière de x .
- Posons $n = \sum_{k=0}^p a_k 10^k$, où $p \in \mathbb{N}$, et $\forall k \in \{0, 1, \dots, p\}$, $a_k \in \{0, 1, \dots, 9\}$, et $a_p \neq 0$. Justifier que $\sigma(n)$ reste inchangé si on permute les chiffres de n .

Partie B : Pour $n \geq 1$, posons $u_n = \frac{\sigma(n+1)}{\sigma(n)}$. Le but de cette partie est l'étude de la convergence de la suite u et la localisation des ses valeurs. On sait que $n = a_p 10^p + \dots + 10a_1 + a_0 = \overline{a_p \dots a_1 a_0}^{10}$

1. Localisation des valeurs de u

- a. Si, au moins, un des chiffres de n n'est pas 9, on note k le plus petit indice tel que $a_k \neq 9$. Alors pour $1 \leq k \leq p-1$, l'entier n s'écrit $n = \overline{a_p \dots a_k 99 \dots 9}^{10}$.

* Montrer que si $k = 0$ alors $\sigma(n+1) = \sigma(n) + 1$. En déduire que $u_n \leq 2$.

** Montrer que si $1 \leq k \leq p-1$ alors $\sigma(n) = a_p + \dots + a_k + 9k$ et $\sigma(n+1) = a_p + \dots + a_k + 1$.

En déduire également que $u_n \leq 2$.

- b. Si tous les chiffres de n sont égaux à 9, calculer $\sigma(n)$ et $\sigma(n+1)$ puis en déduire que $u_n \leq 2$.

c. Montrer que la suite u est bornée.

2. Convergence de la suite u .

- a. Calculer : $\lim_{p \rightarrow +\infty} u_{10^p-1}$ et $\lim_{p \rightarrow +\infty} u_{10^p}$. La suite u est-elle convergente?

- b. Montrer que pour tout entier $n \geq 1$, on a : $1 \leq \sigma(n) \leq 9(1 + \log_{10}(n))$. En déduire la valeur de :

$$\lim_{n \rightarrow +\infty} \sqrt[n]{\sigma(n)}$$

Corrigé**Partie A**

1. On sait que le plus petit entier non nul qui s'écrit avec $p+1$ chiffres est 10^p . Si n est un entier qui s'écrit avec $p+1$ chiffres alors on a : $10^p \leq n < 10^{p+1}$.

2. On a : $10^p \leq n < 10^{p+1} \xRightarrow{\log_{10} \text{ est } \nearrow} p \leq \log_{10}(n) < p+1$, et par suite : $E(\log_{10}(n)) = p$ et donc

le nombre de chiffres de n est $p+1 = 1 + E(\log_{10}(n))$.

3. Si on permute les chiffres de n , on voit de toute évidence que leur somme ne change pas.

Partie B

- 1.a. * Si $k = 0$ alors $n = \overline{a_p \dots a_1 a_0}^{10}$ avec $0 \leq a_0 \leq 8$ et donc : $n+1 = \overline{a_p \dots a_1 (a_0+1)}^{10}$

D'où : $\sigma(n+1) = a_p + \dots + a_1 + (a_0+1) = (a_p + \dots + a_1 + a_0) + 1 = \sigma(n) + 1$

Dans ce cas, on a :

$$u_n = \frac{\sigma(n+1)}{\sigma(n)} = \frac{\sigma(n)+1}{\sigma(n)} = 1 + \frac{1}{\sigma(n)} \leq 1 + 1 = 2$$

- ** Si $1 \leq k \leq p-1$, alors n s'écrit $n = \overline{a_p \dots a_k 99 \dots 9}^{10}$ (k chiffres 9) et donc :

$$n+1 = \overline{a_p \dots (a_k+1) 00 \dots 0}^{10} \quad (k \text{ chiffres } 0)$$

Et donc $\sigma(n) = a_p + \dots + a_k + 9k$ et $\sigma(n+1) = a_p + \dots + a_k + 1$. D'où :

$$u_n = \frac{\sigma(n+1)}{\sigma(n)} = \frac{a_p + \dots + a_k + 1}{a_p + \dots + a_k + 9k} \leq \frac{a_p + \dots + a_k + 1}{a_p + \dots + a_k + 1} = 1 \leq 2$$

- b. Si tous les chiffres de n sont égaux à 9 alors n et $n+1$ s'écrivent :

$$n = \overline{9 \dots 999 \dots 9}^{10} \quad (p+1 \text{ chiffres } 9) \quad \text{et} \quad n+1 = \overline{1 \dots 000 \dots 0}^{10} \quad (1 \text{ chiffre } 1 \text{ et } p+1 \text{ chiffres } 0)$$

D'où : $\sigma(n) = 9(p+1)$ et $\sigma(n+1) = 1$ et donc :

$$u_n = \frac{\sigma(n+1)}{\sigma(n)} = \frac{1}{9(p+1)} \leq 2$$

- c. D'après les questions 1.a. et 1.b., on déduit que dans tous les cas $u_n \leq 2$.

Donc la suite u est bornée : $\forall n \in \mathbb{N}^*, 0 \leq u_n \leq 2$.

- 2.a. Pour $p \geq 1$, on a :

$$\left\{ \begin{array}{l} \sigma(10^p) = \sigma\left(\frac{10 \dots 000 \dots 0}{p \text{ chiffres } 0}\right)^{10} = 1 \\ \sigma(10^p - 1) = \sigma\left(\frac{99 \dots 999 \dots 9}{p \text{ chiffres } 9}\right)^{10} = 9p \\ \sigma(10^p + 1) = \sigma\left(\frac{10 \dots 000 \dots 1}{p-1 \text{ chiffres } 0}\right)^{10} = 2 \end{array} \right.$$

D'où :

$$u_{10^p} = \frac{\sigma(10^p + 1)}{\sigma(10^p)} = \frac{2}{1} = 2 \quad \text{et} \quad u_{10^p - 1} = \frac{\sigma(10^p)}{\sigma(10^p - 1)} = \frac{1}{9p}$$

Donc :

$$\lim_{p \rightarrow +\infty} u_{10^p} = 2 \quad \text{et} \quad \lim_{p \rightarrow +\infty} u_{10^p - 1} = 0$$

La suite u est divergente car on peut en extraire deux suites convergentes de limites différentes.

b. L'entier n s'écrit avec $p + 1$ chiffres tous inférieurs ou égaux à 9. Donc la somme de ses chiffres $\sigma(n)$ vérifie $\sigma(n) \leq 9(p + 1)$. D'autre part, il est évident que $\sigma(n) \geq 1$ car $n \geq 1$. D'où :

$$1 \leq \sigma(n) \leq 9(1 + E(\log_{10}(n))) \quad \text{car} \quad p = E(\log_{10}(n))$$

Et comme $E(\log_{10}(n)) \leq \log_{10}(n)$, on peut écrire enfin : $1 \leq \sigma(n) \leq 9(1 + \log_{10}(n))$.

La fonction $x \mapsto \sqrt[n]{x}$ étant strictement croissante sur $[1; +\infty[$, l'inégalité $1 \leq \sigma(n) \leq 9(1 + \log_{10}(n))$ se transforme en :

$$1 \leq \sqrt[n]{\sigma(n)} \leq \sqrt[n]{9(1 + \log_{10}(n))}$$

On sait que : $\sqrt[n]{9(1 + \log_{10}(n))} = \exp\left[\frac{1}{n} \ln(9(1 + \log_{10}(n)))\right] = \exp\left[\frac{1}{n} [\ln 9 + \ln(1 + \log_{10}(n))]\right]$.

D'autre part, on a :

$$\frac{1}{n} \ln(1 + \log_{10}(n)) = \frac{1}{n} \ln\left(1 + \frac{\ln(n)}{\ln(10)}\right) = \frac{\ln\left(1 + \frac{\ln(n)}{\ln(10)}\right)}{1 + \frac{\ln(n)}{\ln(10)}} \times \left(\frac{1}{n} + \frac{1}{\ln(10)} \times \frac{\ln(n)}{n}\right) \xrightarrow[n \rightarrow +\infty]{} 0$$

$$\text{D'où : } \lim_{n \rightarrow +\infty} \exp\left[\frac{1}{n} \ln(9(1 + \log_{10}(n)))\right] = 1$$

Donc en appliquant le théorème des gendarmes, on conclut que :

$$\lim_{n \rightarrow +\infty} \sqrt[n]{\sigma(n)} = 1$$

Exercice 107

Le mille-pattes ne s'arrête pas pour une patte boiteuse.

Dans cet exercice, on appelle numéro du jour de naissance le rang de ce jour dans le mois et numéro du mois de naissance, le rang du mois dans l'année.

Par exemple, pour une personne née le 14 mai, le numéro du jour de naissance est 14 et le numéro du mois de naissance est 5.

Partie A : Lors d'une représentation, un magicien demande aux spectateurs d'effectuer le programme de calcul (A) suivant :

« Prenez le numéro de votre jour de naissance et multipliez-le par 12.

Prenez le numéro de votre mois de naissance et multipliez-le par 37.

Ajoutez les deux nombres obtenus.

Je pourrai alors vous donner la date de votre anniversaire ».

Un spectateur annonce 308 et en quelques secondes, le magicien déclare : « Votre anniversaire tombe le 1^{er} août ! ».

1. Vérifier que pour une personne née le 1^{er} août, le programme (A) donne effectivement le nombre 308.

2. a. Pour un spectateur donné, on note j le numéro de son jour de naissance, m celui de son mois de naissance et z le résultat obtenu en appliquant le programme de calcul (A).

Exprimer z en fonction de j et de m et démontrer que z et m sont congrus modulo 12.

b. Retrouver alors la date de l'anniversaire d'un spectateur ayant obtenu le nombre 474 en appliquant le programme de calcul (A).

Partie B : Lors d'une autre représentation, le magicien décide de changer son programme de calcul (programme B) : pour un spectateur dont le numéro du jour de naissance est j et le numéro du mois de naissance est m , le magicien demande de calculer le nombre z défini par $z = 12j + 31m$. Dans les questions suivantes, on étudie différentes méthodes permettant de retrouver la date d'anniversaire du spectateur.

1. Première méthode

- Démontrer que les entiers $7m$ et z ont le même reste dans la division euclidienne par 12.
- Pour m variant de 1 à 12, donner le reste de la division euclidienne de $7m$ par 12.
- En déduire la date de l'anniversaire d'un spectateur ayant obtenu le nombre 503 avec le programme (B).

2. Deuxième méthode

- Démontrer que le couple $(-2 ; 17)$ est solution de l'équation diophantienne : $12x + 31y = 503$.
- En déduire que si un couple de relatifs $(x ; y)$ est solution de l'équation : $12x + 31y = 503$, alors on a :

$$12(x + 2) = 31(17 - y).$$

- Déterminer l'ensemble de tous les couples d'entiers relatifs $(x ; y)$, solutions de l'équation :

$$12x + 31y = 503.$$

- Démontrer qu'il existe un unique couple d'entiers relatifs $(x ; y)$ tel que $1 \leq y \leq 12$.

En déduire la date d'anniversaire d'un spectateur ayant obtenu le nombre 503 avec le programme (B).

Corrigé

Partie A

- Pour une personne née le 1^{er} août, le programme de calcul (A) donne 308, en effet :

→ Numéro du jour de naissance multiplié par 12 : $j = 1 \times 12 = 12$;

→ Numéro du mois de naissance multiplié par 37 : $m = 8 \times 37 = 296$;

→ $m + j = 12 + 296 = 308$.

- Pour un spectateur donné, on note j le numéro de son jour de naissance, m celui de son mois de naissance et z le résultat obtenu en appliquant le programme de calcul (A) :

$$z = 12j + 37m, \text{ or } 12j \equiv 0 [12] \text{ et donc } z = 12j + 37m \equiv 37m [12].$$

- Date de l'anniversaire d'un spectateur ayant obtenu le nombre 474 en appliquant le programme de calcul (A) :

$$\begin{cases} z = 474 = 39 \times 12 + 6 \\ z = 37m [12] \end{cases} \Rightarrow z = (3 \times 12 + 1)m \equiv 6 [12]$$

$$\Rightarrow z \equiv 6 [12], \text{ le mois est donc juin.}$$

Donc : $z = 474 = 12j + 37 \times 6 \Rightarrow 12j = 474 - 37 \times 6 = 252 = 21 \times 12 \Rightarrow j = 21$. Il est donc né un 21 juin.

Partie B

1. Première méthode :

- On sait que pour tout entier a , $12a \equiv 0 [12]$ et donc :

$$z = 12j + 31m \equiv 31m [12]; \text{ or } 31m = (2 \times 12 + 7)m \equiv 7m [12] \text{ d'où :}$$

$7m$ et z ont le même reste dans la division euclidienne par 12.

- Le tableau suivant donne le reste de la division euclidienne de $7m$ par 12 pour m variant de 1 à 12 :

m	1	2	3	4	5	6	7	8	9	10	11	12
reste	7	2	9	4	11	6	1	8	3	10	5	0

On remarque qu'à chacun des 12 restes possibles correspond un seul mois.

- Date de l'anniversaire d'un spectateur ayant obtenu le nombre 503 avec le programme de calcul (B) :

$$\begin{cases} z = 503 = 41 \times 12 + 11 \\ z \equiv 7m [12] \end{cases} \Rightarrow 7m \equiv 11 [12]$$

Or dans le tableau précédent, la seule valeur de m qui donne $7m \equiv 11 [12]$ est $m = 5$. Donc le mois est mai. D'autre part : $z = 503 = 12j + 31 \times 5 \Rightarrow 12j = 503 - 31 \times 5 = 29 \times 12 \Rightarrow j = 29$.

Le spectateur est donc né un 29 mai.

2. Deuxième méthode :

a. On vérifie facilement que le couple $(-2; 17)$ est solution de l'équation diophantienne $12x + 31y = 503$.

b. Si un couple $(x; y)$ est solution de l'équation $12x + 31y = 503$ alors :

$$\begin{cases} 12x + 31y = 503 \\ 12 \times (-2) + 31 \times 17 = 503 \end{cases} \xrightarrow{\text{par différence}} 12(x + 2) + 31(y - 17) = 0$$

D'où : (E) $12(x + 2) = 31(17 - y)$.

c. Résolution de l'équation $12x + 31y = 503$:

→ directement :

On vient de voir que $12x + 31y = 503 \Rightarrow 12(x + 2) = 31(17 - y)$

On peut conclure que 12 divise $31(17 - y)$ et comme $12 \wedge 31 = 1$ alors 12 divise $17 - y$ c'est-à-dire qu'il existe un entier relatif k tel que $17 - y = 12k$ et donc $y = 17 - 12k$. En remplaçant y par $17 - 12k$ dans (E), on obtient :

$$\begin{cases} 12(x + 2) = 31(17 - y) \\ y = 17 - 12k \end{cases} \Rightarrow 12(x + 2) = 31 \times 12k \Rightarrow x + 2 = 31k$$

Soit $x = -2 + 31k$.

→ Réciproquement :

Pour tout entier relatif k , on a :

$$12(-2 + 31k) + 31(17 - 12k) = \underbrace{12 \times (-2) + 31 \times 17}_{503} + 12 + 31k - 12 - 31k = 503$$

Donc l'ensemble des solutions de l'équation $12x + 31y = 503$ est :

$$\{(-2 + 31k; 17 - 12k) / k \in \mathbb{Z}\}.$$

d. Cherchons les couples $(x; y) = (-2 + 31k; 17 - 12k)$ tels que $1 \leq y \leq 12$:

$$1 \leq y \leq 12 \Leftrightarrow 1 \leq 17 - 12k \leq 12 \Leftrightarrow 5 \leq 12k \leq 16 \Leftrightarrow \frac{5}{12} \leq k \leq \frac{16}{12}.$$

Comme entre $\frac{5}{12}$ et $\frac{16}{12}$, il y a un seul entier : 1, alors pour $k = 1$, l'équation admet l'unique solution :

$(x; y) = (-2 + 31 \times 1; 17 - 12 \times 1) = (29; 5)$. Donc le spectateur est né un 29 mai.

Exercice 108

Ce qu'un homme ne dit pas est le sel de la conversation.

Le but de cet exercice est de montrer que :

$$\forall n \geq 3, \quad \pi(2n + 1) \geq \ln(2) \times \frac{2n + 1}{\ln(2n + 1)}$$

où $\pi(x)$ désigne le nombre d'entiers premiers inférieurs ou égaux à x .

1. Soient n et p deux entiers naturels. On pose :

$$I_{p,n} = \int_0^1 x^p (1 - x)^n dx$$

a. Calculer $I_{p,0}$ et $I_{p,1}$.

b. Calculer $I_{0,n}$ et en déduire $I_{1,n}$.

c. Établir, pour $n \geq 1$, la relation :

$$I_{p,n} = \frac{n}{p+1} I_{p+1,n-1}$$

En déduire que

$$I_{p,n} = \frac{n! p!}{(n + p + 1)!}$$

d. Calculer $I_{n,n}$ en utilisant la formule du binôme Newton pour le développement de $(1 - x)^n$ puis en déduire l'égalité :

$$\frac{(n!)^2}{(2n + 1)!} = \sum_{k=0}^n \frac{(-1)^k C_n^k}{n + k + 1}$$

2.a. Soit D_n le PPCM des entiers $n + 1, n + 2, \dots, 2n + 1$.

Montrer qu'il existe un entier naturel $a \geq 1$ tel que :

$$\sum_{k=0}^n \frac{(-1)^k C_n^k}{n+k+1} = \frac{a}{D_n}$$

b. En déduire que $D_n \geq \frac{(2n+1)!}{(n!)^2}$.

c. Soit $D_n = \prod_{i=1}^k p_i^{\alpha_i}$ la décomposition en facteurs premiers de D_n .

Justifier que pour tout i compris entre 1 et k , $p_i^{\alpha_i}$ divise l'un des entiers $n+1, n+2, \dots, 2n+1$.

En déduire que $p_i^{\alpha_i} \leq 2n+1$ puis que $k \leq \pi(2n+1)$.

3.a. Montrer que $D_n \leq (2n+1)^{\pi(2n+1)}$.

b. Montrer par récurrence que pour tout naturel $n \geq 3$:

$$\frac{(2n+1)!}{(n!)^2} \geq 2^{2n+1}$$

c. En déduire la minoration annoncée en début de l'exercice.

Corrigé

1.a. Calcul $I_{p,0}$ et $I_{p,1}$:

$$\rightarrow I_{p,0} = \int_0^1 x^p dx = \left[\frac{x^{p+1}}{p+1} \right]_0^1 = \frac{1}{p+1}$$

$$\rightarrow I_{p,1} = \int_0^1 x^p (1-x) dx = \int_0^1 (x^p - x^{p+1}) dx = \int_0^1 x^p dx - \int_0^1 x^{p+1} dx = I_{p,0} - I_{p+1,0} = \frac{1}{p+1} - \frac{1}{p+2}$$

b. Calcul de $I_{0,n}$ et $I_{1,n}$:

$$\rightarrow I_{0,n} = \int_0^1 (1-x)^n dx = \left[-\frac{(1-x)^{n+1}}{n+1} \right]_0^1 = \frac{1}{n+1}$$

$$\rightarrow I_{1,n} = \int_0^1 x(1-x)^n dx = \int_0^1 (x-1+1)(1-x)^n dx = \int_0^1 (1-x)^n dx - \int_0^1 (1-x)^{n+1} dx = I_{0,n} - I_{0,n+1}$$

$$\text{Donc : } I_{1,n} = \frac{1}{n+1} - \frac{1}{n+2}$$

c. La relation $I_{p,n} = \frac{n}{p+1} I_{p+1,n-1}$:

Dans $I_{p,n} = \int_0^1 x^p (1-x)^n dx$, posons : $u'(x) = x^p$ et $v(x) = (1-x)^n$.

Donc : $u(x) = \frac{x^{p+1}}{p+1}$ et $v'(x) = -n(1-x)^{n-1}$ et par suite :

$$I_{p,n} = \left[\frac{x^{p+1}}{p+1} (1-x)^n \right]_0^1 + \frac{n}{p+1} \int_0^1 x^{p+1} (1-x)^{n-1} dx = \frac{n}{p+1} I_{p+1,n-1}$$

Déduction de la formule : $I_{p,n} = \frac{n!p!}{(n+p+1)!}$

On a :

$$\begin{aligned} I_{p,n} &= \frac{n}{p+1} I_{p+1,n-1} \\ I_{p+1,n-1} &= \frac{n-1}{p+2} I_{p+2,n-2} \\ &\dots \dots \dots \frac{2}{p+n-1} I_{p+n-1,1} \\ I_{p+n-1,1} &= \frac{1}{p+n} I_{p+n,0} \end{aligned}$$

Soit, après une multiplication télescopique, on obtient : $I_{p,n} = \frac{n}{p+1} \times \frac{n-1}{p+2} \times \dots \times \frac{1}{p+n} I_{p+n,0}$

Or $I_{p+n,0} = \frac{1}{p+n+1}$, d'où, en multipliant les numérateur et dénominateur par $p!$, on trouve le résultat demandé :

$$I_{p,n} = \frac{n!p!}{(n+p+1)!}$$

d. Calcul de $I_{n,n}$

→ 1^{ère} méthode : En prenant $p = n$ dans la formule $\frac{n!p!}{(n+p+1)!}$:

$$I_{n,n} = \frac{(n!)^2}{(2n+1)!}$$

→ 2^{ème} méthode : En utilisant le développement :

$$(1-x)^n = \sum_{k=0}^{k=n} C_n^k (-1)^k x^k$$

On a :

$$\begin{aligned} I_{n,n} &= \int_0^1 x^n (1-x)^n dx = \int_0^1 x^n \left(\sum_{k=0}^{k=n} C_n^k (-1)^k x^k \right) dx = \int_0^1 \left(\sum_{k=0}^{k=n} C_n^k (-1)^k x^{n+k} \right) dx \\ &= \sum_{k=0}^{k=n} \int_0^1 C_n^k (-1)^k x^{n+k} dx \end{aligned}$$

$$\text{Donc, on a bien : } I_{n,n} = \sum_{k=0}^{k=n} \frac{(-1)^k C_n^k}{n+k+1}.$$

D'où l'égalité :

$$\frac{(n!)^2}{(2n+1)!} = \sum_{k=0}^{k=n} \frac{(-1)^k C_n^k}{n+k+1}$$

2.a. D_n étant le PPCM des entiers $n+1, n+2, \dots, 2n+1$ qui sont les dénominateurs figurant dans l'expression $\sum_{k=0}^{k=n} \frac{(-1)^k C_n^k}{n+k+1}$, alors $I_{n,n}$ s'écrit sous la forme fractionnaire $\frac{a}{D_n}$ avec a un entier tel que :

$$a \geq 1 \text{ car } I_{n,n} = \frac{(n!)^2}{(2n+1)!} > 0.$$

b. On déduit de la question précédente que : $I_{n,n} = \frac{a}{D_n} \geq \frac{1}{D_n}$ et par suite $D_n \geq \frac{(2n+1)!}{(n!)^2}$

c. On sait que pour tout i compris entre 1 et k , $p_i^{\alpha_i}$ divise D_n , qui lui-même divise $\prod_{k=1}^{k=n+1} (n+k)$ et par suite $p_i^{\alpha_i}$ divise l'un des entiers $n+1, n+2, \dots, 2n+1$. D'où pour tout i compris entre 1 et k , on a l'inégalité : $p_i^{\alpha_i} \leq 2n+1$ ($2n+1$ étant le plus grand des entiers $n+1, n+2, \dots, 2n+1$).

Les entiers p_i étant tous premiers et inférieurs ou égaux à $2n+1$ alors leur nombre k vérifie l'inégalité $k \leq \pi(2n+1)$.

3.a. On sait déjà que pour tout i compris entre 1 et k alors $p_i^{\alpha_i} \leq 2n+1$. D'où :

$$\prod_{i=1}^{i=k} p_i^{\alpha_i} = \prod_{i=1}^{i=k} (2n+1) = (2n+1)^k \leq (2n+1)^{\pi(2n+1)}$$

Soit : $D_n \leq (2n+1)^{\pi(2n+1)}$.

b. Soit la propriété P_n : $\ll \forall n \geq 3, \frac{(2n+1)!}{(n!)^2} \geq 2^{2n+1} \gg$

→ $n = 3$, $\frac{(2 \times 3 + 1)!}{(3!)^2} = 140 \geq 2^{2 \times 3 + 1}$, donc P_3 est vraie

→ On suppose qu'il existe un rang n tel que $\frac{(2n+1)!}{(n!)^2} \geq 2^{2n+1}$ est vraie.

Montrons que $\frac{[2(n+1)+1]!}{[(n+1)!]^2} \geq 2^{2(n+1)+1}$. On a :

$$\frac{[2(n+1)+1]!}{[(n+1)!]^2} = \frac{(2n+3)!}{[(n+1)!]^2} = \frac{(2n+1)!}{(n!)^2} \times \frac{(2n+2)(2n+3)}{(n+1)^2}$$

$$\text{Or, on sait que : } \frac{(2n+2)(2n+3)}{(n+1)^2} = \frac{2n+2}{n+1} \times \frac{2n+3}{n+1} \leq 2 \times 2 = 2^2$$

Et selon l'hypothèse de récurrence :

$$\frac{(2n+1)!}{(n!)^2} \geq 2^{2n+1}$$

$$D'où : \frac{[2(n+1)+1]!}{[(n+1)!]^2} \geq 2^{2n+1} \times 2^2 = 2^{2(n+1)+1}$$

Et enfin la propriété est vraie pour tout n supérieur ou égal à 3.

c. On vient de démontrer dans les questions précédentes que pour tout $n \geq 3$, on a :

$$(2n+1)^{\pi(2n+1)} \geq D_n \geq \frac{(2n+1)!}{(n!)^2} \geq 2^{2n+1}$$

Et donc : $(2n+1)^{\pi(2n+1)} \geq 2^{2n+1}$

Comme la fonction : $x \mapsto \ln(x)$ est strictement croissante sur $]0; +\infty[$ alors :

$$\pi(2n+1) \times \ln(2n+1) \geq (2n+1) \times \ln(2)$$

$\ln(2n+1)$ étant strictement positif ($2n+1 \geq 7$) alors l'inégalité énoncée en début de l'exercice s'en déduit :

$$\pi(2n+1) \geq \ln(2) \times \frac{2n+1}{\ln(2n+1)}.$$

Exercice 109	Quand tous les épis lourds de grains mûrs baissent la tête, celui qui reste droit et qui se fait remarquer, c'est l'épi vide.
---------------------	--

On considère le nombre $A = 4444^{4444}$.

1. Question préliminaire :

On note N un entier naturel et S la somme de ses chiffres (dans son écriture en base dix).

Démontrer que $N \equiv S [9]$.

2.a. Déterminer suivant les valeurs de l'entier naturel n le reste de la division euclidienne de 7^n par 9.

b. Prouver que $A \equiv 7 [9]$.

3. On nomme :

→ B la somme des chiffres de A .

→ C la somme des chiffres de B .

→ D la somme des chiffres de C .

a. Sachant que $4444 < 10000$, démontrer que A s'écrit en base dix, avec au plus 20000 chiffres.

b. En déduire que $B \leq 180000$.

c. Prouver que $C \leq 54$.

d. En étudiant la liste des entiers inférieurs à 54, proposer un majorant de D inférieur à 15.

e. En déduire la valeur de D .

Corrigé

1. Question préliminaire :

Soit $\overline{a_n a_{n-1} \dots a_2 a_1 a_0}^{10}$ l'écriture de N en base dix c'est-à-dire que :

$$N = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_2 \times 10^2 + a_1 \times 10 + a_0.$$

Or $10 \equiv 1 [9]$ et pour tout $n \in \mathbb{N}$, on a $10^n \equiv 1 [9]$.

On a donc : $N \equiv a_n + a_{n-1} + \dots + a_2 + a_1 + a_0 [9]$, d'où : $N \equiv S [9]$.

2.a. On a : $7^2 = 49 \equiv 4 [9]$, $7^3 \equiv 7 \times 4 [9] \equiv 28 [9] \equiv 1 [9]$.

Or pour tout $n \in \mathbb{N}$, il existe $k \in \mathbb{N}$ tel que $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$.

→ Si $n = 3k$ alors $7^n = (7^3)^k \equiv 1^k [9] \equiv 1 [9]$.

→ Si $n = 3k + 1$ alors $7^n = (7^3)^k \times 7 \equiv 1^k \times 7 [9] \equiv 7 [9]$.

→ Si $n = 3k + 2$ alors $7^n = (7^3)^k \times 7^2 \equiv 1^k \times 4 [9] \equiv 4 [9]$.

b. On a : $4444 \equiv 7 [9]$ donc $A = 4444^{4444} \equiv 7^{4444} [9]$. Or $4444 = 3 \times 1481 + 1$ donc : $A \equiv 7 [9]$.

3.a. On a : $4444^{4444} < 10000^{4444}$ car la fonction $x \mapsto x^{4444}$ est croissante sur $\mathbb{R}^+$. De plus, on a les inégalités : $10000^{4444} < 10000^{5000} = 10^{20000}$.

Donc $A < 10^{20000}$ et par conséquent A comporte au plus 20000 chiffres.

b. On sait que si $A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_2 \times 10^2 + a_1 \times 10 + a_0$ alors :

$$B = a_n + a_{n-1} + \dots + a_2 + a_1 + a_0.$$

Or pour tout $n \in \mathbb{N}$, on a $a_n \leq 9$ et $n \leq 20000$ donc $B \leq 9 \times 20000 = 180000$.

c. Comme $B \leq 180000$ alors B a au max. 6 chiffres tous inférieurs ou égaux à 9 et donc $C \leq 6 \times 9 = 54$.

d. C est un nombre d'au plus deux chiffres dont le chiffre des dizaines est inférieur ou égal à 5 et celui des unités à 9. Donc : $D \leq 5 + 9 = 14$.

e. On a $A \equiv B [9]$ et $B \equiv C [9]$ et $C \equiv D [9]$. On peut donc en conclure que $A \equiv D [9]$. Or $A \equiv 7 [9]$ et donc $D \equiv 7 [9]$. Comme $1 \leq D \leq 14$ et que le seul entier compris entre 1 et 14 qui soit congru à 7 modulo 9 est 7 lui-même alors on peut conclure que $D = 7$.

Exercice 110

Les erreurs sont les portes de la découverte.

Le théorème de Liouville



Joseph Liouville (1809-1882)

Soit $n \in \mathbb{N}^*$. On se propose de démontrer que l'équation (E) d'inconnue p : $(p-1)! + 1 = p^n$ ne possède pas de solution où p est un entier naturel premier, $p > 5$ (théorème de Liouville, 1844).

1. Montrer que si p est un entier naturel premier tel que $p > 5$, alors $(p-1)^2$ divise $(p-1)!$.

2. On suppose que p est un entier naturel premier tel que $p > 5$, et que p est une solution de (E).

a. Montrer que $p-1$ divise $p^{n-1} + p^{n-2} + \dots + p + 1$.

b. Montrer, d'autre part, que $p^{n-1} + p^{n-2} + \dots + p + 1$ et n ont le même reste dans la division euclidienne par $p-1$.

c. En déduire que $p-1$ divise n .

d. Montrer que $(p-1)^{p-1} < p^n$, puis que $(p-1)! + 1 < p^n$. Conclure.

Corrigé

1. $(p-1)^2$ divise $(p-1)!$.

Il est clair déjà que, par définition d'une factorielle, $p-1$ divise $(p-1)!$.

Tout le problème est donc de démontrer que $(p-2)!$ est divisible par $p-1$.

Mais si p est un entier naturel premier strictement plus grand que 5, il est impair, donc $(p-1)$ est pair.

Donc $\frac{p-1}{2}$ est un entier, strictement plus petit que $p-2$ et différent de 2, puisque $p > 5$.

Dans ces conditions, $(p-2)!$ est divisible par $2 \times \frac{p-1}{2}$, donc par $p-1$.

Si p est un entier naturel premier, $p > 5$, $(p-1)^2$ divise $(p-1)!$.

$$(p-2)! \equiv 0 \pmod{(p-1)}$$

2. a. $p-1$ divise $p^{n-1} + p^{n-2} + \dots + p + 1$.

Si p est solution de (E), on ne peut pas avoir $n = 0$, sinon, il faudrait que $(p-1)! = 0$, ce qui n'est pas possible.

Nécessairement, n est supérieur ou égal à 1.

$$(p-1)! = p^{n-1} - 1 = (p-1)(p^{n-1} + p^{n-2} + \dots + p + 1).$$

On peut simplifier par $p-1$, qui n'est pas nul, puisque p est premier et plus grand que 5.

$$(p-2)! = p^{n-1} + p^{n-2} + \dots + p + 1$$

Or, on a démontré dans la question 1 que $(p-2)!$ était divisible par $p-1$ si p est premier supérieur à 5.

Donc : $p-1$ divise $p^{n-1} + p^{n-2} + \dots + p + 1$.

C'est-à-dire $p^{n-1} + p^{n-2} + \dots + p + 1 \equiv 0 \pmod{(p-1)}$.

b. Reste modulo $p-1$.

$$p \equiv 1 \pmod{(p-1)} \Rightarrow p^{n-1} + p^{n-2} + \dots + p + 1 \equiv 1 + 1 + \dots + 1 \text{ (n fois)} \pmod{(p-1)}$$

Soit $p^{n-1} + p^{n-2} + \dots + p + 1 \equiv n \pmod{(p-1)}$.

c. $p-1$ divise n .

On a déjà établi, en 2.a., que : $p^{n-1} + p^{n-2} + \dots + p + 1 \equiv 0 \pmod{(p-1)}$ et en 2.c. :

$$p^{n-1} + p^{n-2} + \dots + p + 1 \equiv n \pmod{(p-1)}.$$

D'où : $n \equiv 0 \pmod{(p-1)}$ c'est-à-dire que $p-1$ divise n .

d. Inégalité $(p-1)! + 1 < p^n$

Si $p-1$ divise n , c'est que $p-1$ est inférieur à n .

Or l'exponentiation : $x \mapsto x^{p-1}$ est une application strictement croissante sur $[1; +\infty[$:

$$p-1 < p \Rightarrow (p-1)^{p-1} < p^{p-1} \leq p^n$$

On a donc bien : $(p-1)^{p-1} < p^n$.

Or les $p-1$ facteurs, de 1 à $p-1$, qui entrent dans $(p-1)!$ sont tous inférieurs ou égaux à $p-1$ et il y en a au moins un qui est strictement plus petit que $p-1$, puisque p est supérieur à 5.

Donc $(p-1)!$ est strictement plus petit que $(p-1)^{p-1}$ donc $(p-1)! + 1$ est inférieur ou égal au nombre $(p-1)^{p-1}$. Donc : $(p-1)! + 1 < p^n$.

Cette inégalité contredit le fait que p vérifie l'équation (E) : $(p-1)! + 1 = p^n$.

En conclusion : L'équation (E) : $(p-1)! + 1 = p^n$ ne possède pas de solution où p est un entier naturel premier tel que $p > 5$.

Exercice 111

Le sage parle des idées, l'intelligent des faits, le vulgaire de ce qu'il mange.

Théorème du reste chinois généralisé

Soient m et n deux entiers naturels premiers entre eux et supérieurs ou égaux à 2.

1.a. Démontrer que pour tous entiers relatifs a et b , il existe deux entiers relatifs u et v tels que :

$$b + (a-b)vn = a + (b-a)um.$$

b. En déduire que le système (1) $\begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases}$ admet au moins une solution dans l'ensemble $\mathbb{Z}$.

2.a. Démontrer que si x et y sont des entiers relatifs solutions du système (1) alors l'entier $x - y$ est multiple de m et de n .

b. En déduire si x est solution de (1) alors tout entier y tel que $y \equiv x [mn]$ est également solution du (1) dans $\mathbb{Z}$.

3. Soient k entiers naturels $n_1, n_2, \dots, n_k$ premiers entre eux deux à deux et k entiers $r_1, r_2, \dots, r_k$.

On note (S) le système de congruences
$$\begin{cases} x \equiv r_1 [n_1] \\ x \equiv r_2 [n_2] \\ \vdots \\ x \equiv r_k [n_k] \end{cases}$$

Démontrer qu'il existe $u_1, u_2, \dots, u_k$ dans $\mathbb{Z}$ tels que :

$$x \equiv r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_k N_k u_k [n_1 \times n_2 \times \dots \times n_k]$$

avec pour tout $p \in \llbracket 1; k \rrbracket$:

$$N = \frac{n_1 \times n_2 \times \dots \times n_k}{n_p} = n_1 \times n_2 \times \dots \times n_{p-1} \times n_{p+1} \times \dots \times n_k$$

Application :

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Survient alors un naufrage et seuls 6 pirates, le cuisinier et le trésor sont sauvés et le partage laisserait 5 pièces d'or à ce dernier. On cherche alors à déterminer la fortune minimale que peut espérer ce dernier s'il décide d'empoisonner le reste des pirates.

1. On note x la fortune que peut espérer ce dernier s'il décide d'empoisonner le reste des pirates.

Démontrer qu'il existe u_1, u_2, u_3 et k dans $\mathbb{Z}$ tels que :

$$x = 198u_1 + 408u_2 + 935u_3 + 1122k$$

2. Trouver a et b dans $\mathbb{Z}$ tels que $17a + 66b = 1$ et en déduire u_1 .

3. De la même façon, trouver u_2 et u_3 .

4. En déduire que $x = 4151 + 1122k$.

5. Répondre au problème.

Corrigé

1.a. Les entiers m et n étant premiers entre eux, le théorème de Bézout nous permet de dire qu'il existe deux entiers relatifs u et v tels que $um + vn = 1$. Dans ce cas, on a :

$(a-b)um + (a-b)vn = a-b$; ce qui peut s'écrire également : $b + (a-b)vn = a + (b-a)um$.

b. En posant $x = b + (a-b)vn = a + (b-a)um$, on vérifie facilement que : $x \equiv a [m]$ et $x \equiv b [n]$ et donc x est bien solution du système (1).

2.a. Soit x et y deux solutions du système (1).

On a : d'une part, $x \equiv a [m]$ et $y \equiv a [m]$ donc $y - x \equiv 0 [m]$ et d'autre part, $x \equiv b [n]$ et $y \equiv b [n]$ donc $y - x \equiv 0 [n]$.

Or $y - x \equiv 0 [m]$ signifie $m | y - x$ comme $y - x \equiv 0 [n]$ signifie $n | y - x$ et sachant que m et n sont premiers entre eux alors le théorème de Gauss permet de conclure que $m \times n | y - x$ c'est-à-dire que $y - x \equiv 0 [mn]$.

b. Si x est une solution du système (1) alors d'après la question précédente, toute autre solution y est telle que : $y - x \equiv 0 [mn]$ et donc $y \equiv x [mn]$.

3. Démontrons que $x \equiv r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_k N_k u_k [n_1 \times n_2 \times \dots \times n_k]$ est une solution du système. On sait que pour tout $i \in \llbracket 1; k \rrbracket$, on a $\text{PGCD}(N_i, n_i) = 1$. Donc d'après le théorème de Bézout, il existe u_i et v_i tels que : $u_i N_i + v_i n_i = 1$.

On a :

$$\begin{aligned} r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_k N_k u_k &= r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_i N_i u_i + \dots + r_k N_k u_k \\ &= r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_i (1 - v_i n_i) + \dots + r_k N_k u_k \\ &= r_i + r_1 N_1 u_1 + r_2 N_2 u_2 + \dots - r_i v_i n_i + \dots + r_k N_k u_k \end{aligned}$$

Or : $r_1 N_1 u_1 + r_2 N_2 u_2 + \dots - r_i v_i n_i + \dots + r_k N_k u_k \equiv 0 [n_i]$ donc pour tout $i \in \llbracket 1, k \rrbracket$, on a :
 $r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_k N_k u_k \equiv r_i [n_i]$.

En conclusion :

L'entier x défini par $x = r_1 N_1 u_1 + r_2 N_2 u_2 + \dots + r_k N_k u_k$ est solution du système (S).

Montrons que toute solution y du système vérifie $y \equiv x [n_1 \times n_2 \times \dots \times n_k]$.

Si y est solution du système alors $y \equiv x [n_i]$ et ceci pour tout $i \in \llbracket 1, k \rrbracket$. Cela signifie, entre autres, que pour tout $i \in \llbracket 1, k \rrbracket$, on a n_i divise $y - x$. Comme les entiers n_i sont premiers entre eux deux à deux alors Gauss nous permet de conclure que :

$$n_1 \times n_2 \times \dots \times n_k \text{ divise } y - x \text{ et donc } y \equiv x [n_1 \times n_2 \times \dots \times n_k].$$

Conclusion : Le système (S) admet, modulo $n_1 \times n_2 \times \dots \times n_k$, une unique solution.

Application :

1. On note x la fortune que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates.

Les données nous suggèrent de chercher le plus petit entier positif x tel que :

$$\begin{cases} x \equiv 3 [17] \\ x \equiv 4 [11] \\ x \equiv 5 [6] \end{cases}$$

D'après les résultats de la question du préambule, il existe u_1, u_2, u_3 de $\mathbb{Z}$ tels que :

$$x \equiv 3 \times 11 \times 6 u_1 + 4 \times 17 \times 6 u_2 + 5 \times 17 \times 11 u_3 [17 \times 11 \times 6]$$

C'est-à-dire que : $x \equiv 198 u_1 + 408 u_2 + 935 u_3 [1122]$. Donc il existe $k \in \mathbb{Z}$ tel que :

$$x = 198 u_1 + 408 u_2 + 935 u_3 + 1122 k.$$

2. Pour déterminer u_1 , on effectue la division euclidienne de 66 par 17 :

$$66 = 3 \times 17 + 15$$

$$17 = 1 \times 15 + 2$$

$$15 = 7 \times 2 + 1$$

On a donc :

$$1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 1 \times 15) = 8 \times 15 - 7 \times 17 = 8 \times (66 - 3 \times 17) - 7 \times 17 = 8 \times 66 - 31 \times 17$$

Enfin $-31 \times 17 + 8 \times 66 = 1$ et on a obtenu $a = -31$ et $b = 8$ et donc on peut conclure que $u_1 = 8$.

3. Pour déterminer u_2 , on effectue la division euclidienne de 102 par 11 :

$$102 = 9 \times 11 + 3$$

$$11 = 3 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

On a donc :

$$\begin{aligned} 1 &= 3 - 1 \times 2 = 3 - 1 \times (11 - 3 \times 3) = 4 \times 3 - 1 \times 11 \\ &= 4 \times (102 - 9 \times 11) - 1 \times 11 = 4 \times 102 - 37 \times 11 \end{aligned}$$

Donc $4 \times 102 - 37 \times 11 = 1$ et selon le théorème chinois $u_2 = 4$.

Pour déterminer u_3 , on divise 187 par 6 et on trouve $1 \times 187 - 31 \times 6 = 1$ et donc $u_3 = 1$.

4. On sait déjà que : $x = 198 u_1 + 408 u_2 + 935 u_3 + 1122 k$ d'où :

$$x = 198 \times 8 + 408 \times 4 + 935 \times 1 + 1122 k \equiv 4151 [1122]$$

5. L'entier 4151 est une solution du système (S). Mais la solution du problème posé est la solution minimale de (S). Or $4151 = 3 \times 1122 + 785$ et donc $4151 \equiv 785 [1122]$. Enfin la réponse au problème est 785 pièces d'or.

Exercice 112	La parole n'a d'autre parure que la vérité.
---------------------	--

C'est plus de la logique que de l'arithmétique

Un problème mathématique posé à des lycéens de Singapour, réputés pour être parmi les plus doués de la planète, a mis en émoi les internautes du monde entier, suscitant débats et contestations. Posé le 8 avril 2015 à des élèves de 15 et 16 ans dans le cadre d'une olympiade de maths, le problème est le suivant: Cheryl veut faire deviner la date de son anniversaire à deux nouveaux amis, Albert et Bernard, en ne leur fournissant que de minces indices.

Cheryl suggère 10 dates: les 15, 16 et 19 mai, les 17 et 18 juin, les 14 et 16 juillet, et les 14, 15 et 17 août. A Albert, elle donne le mois, à Bernard, le jour. A partir d'une courte conversation entre les deux garçons — qui exclut bien sûr les réponses précises de Cheryl –, la logique seule doit ensuite permettre de résoudre ce casse-tête singapourien.

Les organisateurs en ont depuis livré la clé sur le site de **Singapore and Asian Schools Math Olympiad** mais les internautes continuaient de commenter, railler ou contester le libellé et les résultats du problème. « ça n'a aucun sens, vraiment aucun sens », s'agaçait un certain Adam Kelly sur Facebook. Et d'ajouter: « Voici pourquoi vous avez tort ». Également sur Facebook, David Leong, lui, l'a pris avec humour: « Cheryl visiblement ne voulait pas inviter Bernard et Albert à sa fête d'anniversaire », a-t-il plaisanté.

Selon une enquête publiée début avril par l'OCDE (Organisation de Coopération et de Développement Économiques), c'est à Singapour, puis en Corée du Sud, au Japon, à Macao, Hong Kong et Shanghai, que les élèves se débrouillent le mieux en résolution de problèmes, parmi 44 pays ou économies membres de l'organisation internationale.

Si vous voulez vous aussi tenter de relever le défi et muscler un peu vos méninges, voici l'énoncé en français :

Cheryl donne à ses deux amis dix dates possibles de son anniversaire :

les 15, 16 et 19 mai ;

le 17 et 18 juin ;

le 14 et 16 juillet ;

le 14, 15 et 17 août.

Cheryl a ensuite dit à Albert le mois, et à Bernard le jour de son anniversaire.

Albert affirme ensuite :

« Je ne sais pas quand est l'anniversaire de Cheryl mais je sais que Bernard ne sait pas non plus. »

Bernard ajoute :

« Au départ, je ne savais pas quand était l'anniversaire de Cheryl, mais maintenant je sais. »

Albert répond :

« Alors je sais aussi quand est l'anniversaire de Cheryl. »

Bonne chance !

Corrigé

Pour apporter la solution, le quotidien **the Guardian** a fait appel à Alex Bellos, un spécialiste des questions mathématiques. Le site Slate-France a relayé cette solution en français :

– Les dix dates se situent entre le 14 et le 19, sachant que le 18 et le 19 n'apparaissent qu'une seule fois. Si Cheryl était née un 18 ou 19, Bernard aurait pu deviner la date en connaissant juste le jour.

– Mais pourquoi Albert dit-il savoir que Bernard ne sait pas ? Si Cheryl avait dit à Albert être née en mai ou juin, il aurait été possible que son anniversaire soit le 19 mai ou le 18 juin. Donc l'anniversaire de Cheryl est en juillet ou août.

– Comment Bernard connaît-il la date d'anniversaire après qu'Albert a parlé ? Parmi les cinq dates restantes en juillet et août, les dates sont entre 15 et 17 avec uniquement le 14 répété deux fois. Si Cheryl avait dit à Bernard être née le 14, Bernard n'aurait pas pu savoir. Le fait que Bernard dise

savoir implique que son anniversaire n'est pas un 14. Il ne reste donc que trois possibilités : le 16 juillet, le 15 août et le 17 août.

– Après que Bernard s'est exprimé, Albert connaît la date de l'anniversaire. Si Cheryl avait dit à Albert être née en août, alors Albert n'aurait pas pu savoir parce qu'il y a deux dates possibles en août.

Donc Cheryl est née le 16 juillet.

C'est clair ?

Exercice 113[⊗]

La faiblesse de la force est de ne croire qu'à la force.

Décomposition d'un entier selon Zeckendorf



Il s'agit, sur cette photo, d'Édouard Zeckendorf, colonel de l'armée, médecin et mathématicien belge (1901-1983). On sait que tout nombre entier naturel peut s'écrire de manière unique comme produit de puissances de nombres premiers. Le théorème de Zeckendorf donne une autre écriture : tout nombre entier naturel non nul peut s'écrire de manière unique comme somme de nombres de Fibonacci différents et non consécutifs.

Traditionnellement, la suite de Fibonacci commence par : 0; 1; 1; 2; 3; 5; ..., mais comme il s'agit ici de nombres non nuls, nous ferons commencer la suite à 1 : $F_0 = 1; F_1 = 2; F_2 = 3; \dots$, et bien entendu :

$$F_{n+2} = F_{n+1} + F_n.$$

L'objectif de l'exercice est :

- de donner une démonstration de ce théorème qui utilise un résultat préliminaire qui porte sur une propriété des nombres de Fibonacci.
- d'appliquer le résultat du théorème pour développer une stratégie gagnante dans un jeu de société (jeu de Nim).

1. Résultat préliminaire

Soit S un ensemble non vide de nombres de Fibonacci différents et non consécutifs, et soit F_j le plus grand d'entre eux. On a :

$$\sum_S F_j < F_{j+1}$$

2. Théorème de Zeckendorf

Etant donné un entier naturel N strictement positif, il existe un ensemble unique d'entiers positifs ou nuls $c_0, c_1, \dots, c_k$ tels que :

- pour tout $i \in \llbracket 0; k-1 \rrbracket : c_{i+1} > c_i$;
- F_{c_i} est le c_i ème nombre de Fibonacci (en commençant comme il a été dit par $F_0 = 1$) ;
- les entiers c_i et donc les nombres F_{c_i} ne sont pas consécutifs ;
- $N = \sum_{i=0}^k F_{c_i}$.

3. Application : jeu de Nim

Deux joueurs tirent à tour de rôle des allumettes d'une boîte, avec les règles suivantes :

- Chaque joueur tire à chaque fois au moins une allumette.
- Le premier joueur ne retire pas la totalité des allumettes au premier tour.
- Un joueur tire au plus deux fois le nombre d'allumettes tirées par le joueur précédent.
- Le joueur qui retire la dernière allumette a gagné.

Montrer que le premier joueur a une stratégie gagnante si le nombre initial d'allumettes n'est pas un nombre de Fibonacci. Quelle est cette stratégie ? Que dire du cas où le nombre initial d'allumettes est un nombre de Fibonacci ?

⇒ on pourra se servir d'une décomposition dans la base de Fibonacci du nombre d'allumettes, et considérer le plus petit terme de cette décomposition.

Corrigé

1. Démonstration du résultat préliminaire par récurrence sur n , cardinal de S .

→ La propriété est vraie pour $n = 1$: S ne contient alors que F_j et $F_j < F_{j+1}$.

→ Supposons donc que la propriété soit vraie jusqu'à l'ordre n .

Soit alors $S = \{F_{c_0}, \dots, F_{c_l}, F_j\}$ un ensemble à $n + 1$ nombres de Fibonacci différents et non consécutifs. On peut toujours supposer que les éléments sont rangés dans l'ordre croissant :

$$F_{c_0} < \dots < F_l < F_j.$$

Soit $S' = S \setminus \{F_j\}$: S' est un ensemble de n nombres de Fibonacci différents et non consécutifs, dont le plus grand est F_l .

L'hypothèse de récurrence s'applique donc à S' : $\sum_{S'} F_{c_i} < F_{l+1}$.

Mais $F_{l+1} < F_{j-1}$ car F_l et F_j ne sont pas consécutifs.

$$\text{Donc : } \sum_S F_{c_i} = \sum_{S'} F_{c_i} + F_j < F_{j-1} + F_j = F_{j+1}.$$

Le résultat est donc bien établi.

2. Démonstration du théorème

a. Existence

Raisonnons par récurrence sur N .

→ La propriété est triviale pour $N = 1, 2$, ou 3 .

Elle est immédiate pour $N = 4 = 1 + 3$. ($4 = 2 + 2$ ne conviendrait pas car on aurait deux termes égaux).

→ On suppose donc que la propriété est vraie jusqu'à $N - 1$.

Soit alors F_k le plus grand nombre de Fibonacci inférieur ou égal à N : $F_k \leq N < F_{k+1}$.

- Si $F_k = N$, c'est terminé. La somme est constituée du seul terme F_k .
- Si $F_k < N$, soit $M = N - F_k$. On a $M < N$ donc $M \leq N - 1$ (il s'agit d'entiers), et selon l'hypothèse de récurrence, l'énoncé est vrai pour M :

Il existe une suite strictement croissante d'entiers $c_0, c_1, \dots, c_l$ telle que $M = F_{c_0} + F_{c_1} + \dots + F_{c_l}$, et donc $N = F_{c_0} + F_{c_1} + \dots + F_{c_l} + F_k$.

Si F_k était égal à l'un des c_j , c_l étant le plus grand, on aurait $F_k < F_{c_l} \leq M < N$, ce qui contredirait le fait que F_k est le plus grand nombre de Fibonacci inférieur à N .

Donc F_k est supérieur à tous les F_{c_j} (qui sont rangés dans l'ordre croissant).

En outre, il n'est pas consécutif à F_{c_l} sinon on aurait $F_{k+1} = F_{c_l} + F_k$ donc $F_{k+1} \leq M + F_k = N$ ce qui contredirait que $N < F_{k+1}$.

La propriété est donc vraie au rang N , et donc pour tout entier $N \geq 1$.

b. Unicité

Par récurrence sur N .

→ L'écriture est unique pour $N = 1; 2$; ou 3 ; ainsi que pour $N = 4 = 1 + 3$ (pas d'autre possibilité).

→ On suppose donc que l'écriture est unique jusqu'à $N - 1$.

N est une somme de nombres de Fibonacci différents et non consécutifs. S'il admet deux écritures, soit F_j et F_k les éléments maximaux de chacune de ces écritures.

- Si $j = k$, $F_j = F_k$, et donc $M = N - F_j = N - F_k$ qui est inférieur à N admet une écriture unique selon l'hypothèse de récurrence. Il en résulte que c'est également vrai pour N qui s'obtient en ajoutant le même nombre ($F_j = F_k$) à M .
- Si $j \neq k$, par exemple $j < k$, selon le lemme ci-dessus, $N < F_{j+1} \leq F_k \leq N$, ce qui est contradictoire.

L'unicité est réussie, et par suite le théorème est donc établi.

3. Application

On rappelle ici que la suite de Fibonacci est croissante.

• Si le nombre initial d'allumettes n'est pas un nombre de Fibonacci, le joueur 1 peut retirer un nombre d'allumettes égal au plus petit nombre de Fibonacci de la décomposition (il retirera ainsi au moins une allumette, et pas la totalité)

• Supposons que lors d'une étape, le joueur 1 retire un nombre d'allumettes égal au plus petit nombre de la décomposition, disons F_{i_1} , où $n = F_{i_1} + F_{i_2} + \dots + F_{i_s}$.

Si $s = 1$, alors il ne reste plus d'allumettes, et le joueur 1 a gagné. Sinon il reste $F_{i_2} + \dots + F_{i_s}$ allumettes. Alors le joueur 2 doit retirer un nombre d'allumettes au plus égal à :

$$2F_{i_1} < F_{i_1} + F_{i_1+1} = F_{i_1+2} \leq F_{i_2}$$

Donc il tire strictement moins de F_{i_2} allumettes. En particulier, il ne peut pas retirer la totalité des allumettes, donc le joueur 2 ne peut pas gagner à cette étape.

• Soit $m < F_{i_2}$ le nombre d'allumettes que le joueur 2 retire, et soit $\ell = F_{i_2} - m$. Soit $2 \leq j_1 < \dots < j_t$ non consécutifs tels que $\ell = F_{j_1} + \dots + F_{j_t}$.

Comme on a $\ell < F_{i_2}$, on a aussi $F_{j_t} < F_{i_2}$, donc $j_t \leq i_2$, donc j_t et i_3 sont non consécutifs, et on a $2 \leq j_1 < \dots < j_t < i_3 < \dots < i_s$, et $n - F_{i_1} - \ell = F_{j_1} + \dots + F_{j_t} + F_{i_3} + \dots + F_{i_s}$.

Il s'agit donc de la décomposition de $n - F_{i_1} - m$, qui est le nombre d'allumettes restant à l'issue du tirage du joueur 2.

• On a $F_{j_1} \leq 2m$. En effet, supposons le contraire :

Soit alors $m = F_{\ell_1} + \dots + F_{\ell_u}$, la décomposition de Zeckendorf de m , où $\ell_1 < \ell_2 < \dots < \ell_u$.

On a alors $F_{\ell_u+1} = F_{\ell_u} + F_{\ell_u-1} \leq 2F_{\ell_u} \leq 2m < F_{j_1}$, par l'hypothèse de la démonstration par l'absurde ; Ainsi, par croissance, $\ell_u + 1 < j_1$. On en déduit que :

$$2 \leq \ell_1 < \dots < \ell_u < j_1 < \dots < j_t$$

est une suite d'indices distincts et non consécutifs, et :

$$F_{i_2} = m + \ell = F_{\ell_1} + \dots + F_{\ell_u} + F_{j_1} + \dots + F_{j_t}$$

ce qui contredit l'unicité de la décomposition de Zeckendorf de F_{j_2} .

• Puisque $F_{j_1} \leq 2m$, le joueur 1 peut tirer F_{j_1} allumettes, donc il se retrouve dans la configuration où il peut tirer un nombre d'allumettes égal au plus petit terme de la décomposition.

• Ainsi, à chaque étape, le joueur 1 peut s'arranger pour tirer le plus petit terme de la décomposition. Ce faisant, d'après ce qui précède, le joueur 2 ne peut jamais gagner. Comme il y a nécessairement un gagnant (car le nombre d'allumettes diminue strictement, on peut voir cela comme une application du principe de la descente infinie), c'est le joueur 1 qui gagne.

• Si le nombre initial d'allumettes est un nombre de Fibonacci, le joueur 1 ne pouvant pas tirer toutes les allumettes, est obligé d'en tirer strictement moins. Il se retrouve donc dans la situation du joueur 2 précédemment, qui se voyait obligé de tirer moins d'allumettes que le plus petit terme dans la décomposition de Fibonacci du nombre d'allumettes restantes. Les rôles sont donc inversés, et c'est maintenant le joueur 2 qui a une stratégie gagnante.

Exercice 114²

Il faut toujours avoir deux idées : l'une pour tuer l'autre.

Formule de Minàc et Willans

Cette formule et sa démonstration ne sont pas exigibles pour le bac. Elles sont juste données à titre culturel et pour le plaisir de faire des maths!!! Elle a plus un intérêt théorique que pratique.

On adopte ici la notation suivante : si $x \in \mathbb{R}$, on note $[x]$ sa partie entière.

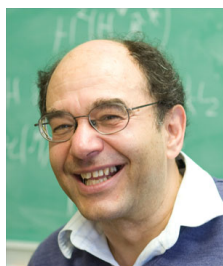


Joseph Bertrand (1822 - 1900)

Le mathématicien français Joseph Bertrand a vérifié, pour tout entier $1 \leq n \leq 3000000$, que l'intervalle $[n; 2n]$ contient toujours au moins un nombre premier. Il a postulé (ou conjecturé) que cela devait être vrai pour tout entier $n \geq 1$, d'où le terme "postulat". Cela a été démontré pour la première fois en 1850. Bien que son postulat soit maintenant démontré, l'usage veut que l'on parle du "postulat de Bertrand".

Théorème (Postulat de Bertrand) : Pour tout entier $n \geq 1$, l'intervalle $[n; 2n]$ contient au moins un nombre premier.

Le but est ici de démontrer le théorème suivant (découvert en 1995 par le mathématicien canadien Jan Minàc) en utilisant le postulat de Bertrand :



Prof. Jan Mináč

Théorème de Mináč et Willans :

Soit $n \geq 1$ un entier. Si p_n est le $n^{\text{ième}}$ nombre premier alors :

$$p_n = 2 + \sum_{m=2}^{2^n} \left\lceil \frac{n}{1 + \sum_{j=2}^m \left[\frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right]} \right\rceil^{\frac{1}{n}}$$

1. Soit $(p_n)_{n \geq 1}$ la suite des nombres premiers ($p_1 = 2, p_2 = 3, \dots$).

En utilisant un raisonnement par récurrence et le postulat de Bertrand, montrer que :

$$\forall n \geq 2; p_n \leq 2^n$$

2. Soit $j \geq 2$ un entier.

a. Montrer qu'il existe des entiers naturels q et r tels que :

$$\frac{(j-1)!}{j} = q + \frac{r-1}{j}, \quad q \geq 0, \quad 0 \leq r < j.$$

b. Montrer que :

- Si $r = 0$ alors $\left\lfloor \frac{(j-1)!}{j} \right\rfloor = q - 1$.
- Si $r > 0$ alors $\left\lfloor \frac{(j-1)!}{j} \right\rfloor = q$.

c. En déduire que :

$$\text{Pour tout entier } j \geq 2, \text{ on a : } \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \begin{cases} 1 & \text{si } j \text{ est premier} \\ 0 & \text{sinon} \end{cases}$$

3. Pour $m \geq 2$ entier, notons $\pi(m)$ le nombre de nombres premiers inférieurs ou égaux à m . Montrer que :

$$\pi(m) = \sum_{j=2}^m \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor.$$

4. Soit $m \geq 2$ un entier.

a. En supposant que $\pi(m) \leq n - 1$, montrer que :

$$1 \leq \left\lfloor \frac{n}{\pi(m) + 1} \right\rfloor \leq n.$$

b. Soit f la fonction définie sur $[1; +\infty[$ par :

$$f(x) = x^{\frac{1}{x}} = \exp\left(\frac{\ln x}{x}\right)$$

Montrer que :

$$\forall x \geq 1, \quad 1 \leq f(x) < 2.$$

En déduire que :

$$\left\lceil \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \right\rceil = 1.$$

c. Montrer que si $\pi(m) > n - 1$ alors :

$$\left\lceil \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \right\rceil = 0.$$

5. Soit S la somme définie par :

$$S = \sum_{m=2}^{2^n} \left\lceil \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \right\rceil$$

Justifier que $S = p_n - 2$ puis en déduire la formule annoncée à l'amorce de l'exercice.

Corrigé

1. Pour $n \geq 2$, soit $P(n)$ la proposition suivante : $P(n) : p_n \leq 2^n$

La proposition $P(n)$ est vraie pour $n = 2$. En effet : $p_2 = 3 \leq 4 = 2^2$.

Fixons un entier $n \geq 2$ et supposons $P(n)$ vraie, i.e.

$$p_n \leq 2^n \text{ (H.R.)}.$$

Montrons que $P(n+1)$ est vraie, i.e.

$$p_{n+1} \leq 2^{n+1}$$

En effet, par le postulat de Bertrand, l'intervalle $]p_n; 2p_n]$ contient au moins un nombre premier. En particulier, le nombre premier suivant p_n , i.e. p_{n+1} est dans cet intervalle, i.e.

$$p_{n+1} \leq 2p_n$$

L'H.R. permet alors d'écrire : $p_{n+1} \leq 2 \times 2^n = 2^{n+1}$, cqfd.

La proposition $P(n)$ est donc héréditaire et vraie pour $n = 1$, donc est vraie pour tout entier $n \geq 1$.

2. Soit $j \geq 2$ un entier.

a. Effectuons la division euclidienne de $(j-1)! + 1$ par j :

$$(j-1)! + 1 = qj + r, \quad q \geq 0, \quad 0 \leq r < j$$

Il existe donc des entiers naturels q et r tels que

$$\frac{(j-1)!}{j} = q + \frac{r-1}{j}, \quad q \geq 0, \quad 0 \leq r < j$$

b. On sait qu'il existe deux entiers naturels q et r tels que :

$$(j-1)! + 1 = qj + r, \quad q \geq 0, \quad 0 \leq r < j$$

On remarque que :

- Si $r = 0$ alors $(j-1)! + 1 = qj \equiv 0 [j]$ et donc selon Wilson j est premier.

Dans ce cas, on a :

$$q - 1 \leq \frac{(j-1)!}{j} = q - \frac{1}{j} < q$$

$$\text{donc } \left\lfloor \frac{(j-1)!}{j} \right\rfloor = q - 1.$$

- Si $r > 0$, alors j n'est pas premier (par le théorème de Wilson) ; dans ce cas

$$\frac{(j-1)!}{j} = q + \frac{r-1}{j}, \quad q \geq 0, \quad 0 \leq r-1 < j.$$

Alors :

$$q \leq \frac{(j-1)!}{j} = q + \frac{r-1}{j} < q + 1.$$

$$\text{On a donc } \left\lfloor \frac{(j-1)!}{j} \right\rfloor = q.$$

c. On vient de voir à la question précédente que :

$$\text{si } r = 0 \text{ alors } j \text{ est premier et } \left\lfloor \frac{(j-1)!}{j} \right\rfloor = q - 1 ;$$

$$\text{si } r > 0 \text{ alors } j \text{ n'est pas premier et } \left\lfloor \frac{(j-1)!}{j} \right\rfloor = q.$$

D'où :

Si j est premier alors :

$$\left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \left\lfloor \frac{(j-1)! + 1}{j} - (q-1) \right\rfloor = \lfloor 1 \rfloor = 1;$$

Si j n'est pas premier alors :

$$\left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \left\lfloor \frac{(j-1)! + 1}{j} - q \right\rfloor = \left\lfloor \frac{r-1}{j} \right\rfloor = 0 \text{ car } 0 \leq \frac{r-1}{j} < 1.$$

Donc en conclusion, on a :

$$\text{Pour tout entier } j \geq 2, \text{ on a : } \left\lfloor \frac{(j-1)! + 1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor = \begin{cases} 1 & \text{si } j \text{ est premier} \\ 0 & \text{sinon} \end{cases}.$$

3. Le réel

$$\left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right]$$

vaut 1 si j est premier et 0 sinon. Par conséquent, dans la somme :

$$\sum_{j=2}^m \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right]$$

il y a autant de 1 que de nombres premiers entre 2 et m (i.e. $\pi(m)$) et sinon que des zéros.

On a donc :

$$\pi(m) = \sum_{j=2}^m \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right].$$

4. Soit $m \geq 2$ un entier.

a. Supposons que $\pi(m) \leq n - 1$. On a alors $\pi(m) + 1 \leq n$, donc :

$$\frac{n}{\pi(m) + 1} \geq 1.$$

De plus :

$$\frac{n}{\pi(m) + 1} \leq n.$$

Ainsi :

$$1 \leq \frac{n}{\pi(m) + 1} \leq n \Rightarrow 1 \leq \left[\frac{n}{\pi(m) + 1} \right] \leq n.$$

b. Soit f la fonction définie sur $[1; +\infty[$ par :

$$f(x) = x^{\frac{1}{x}} = \exp\left(\frac{\ln x}{x}\right)$$

La fonction f est dérivable sur $[1; +\infty[$ et on a :

$$\forall x \geq 1, \quad f'(x) = \frac{1 - \ln x}{x^2} \exp\left(\frac{\ln x}{x}\right) \begin{cases} \geq 0 & \text{si } 1 \leq x \leq e \\ \leq & \text{si } x \geq e \end{cases}$$

Donc f présente un maximum en $x = e$ égal à $f(e) = e^{\frac{1}{e}} \cong 1,44 < 2$.

De plus, on a :

$$f(1) = 1 \text{ et } \lim_{x \rightarrow +\infty} f(x) = 1$$

D'où :

$$\forall x \geq 1, \quad 1 \leq f(x) < 2.$$

D'autre part, on sait d'après la question 4.a. que :

$$1 \leq \left[\frac{n}{\pi(m) + 1} \right] \leq n \quad \text{pour } \pi(m) \leq n - 1.$$

La fonction g définie sur $]0; +\infty[$ par $g(x) = x^{\frac{1}{n}}$ étant croissante, il vient :

$$1 \leq \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \leq n^{\frac{1}{n}} = f(n)$$

Or, on vient d'établir que $\forall x \geq 1, 1 \leq f(x) < 2$, d'où $f(n) < 2$ pour tout entier $n \geq 1$.

$$\text{Donc : } 1 \leq \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} < 2.$$

Et par suite :

$$\left[\left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \right] = 1.$$

c. On suppose que $\pi(m) > n - 1$.

Dans ce cas,

$$\begin{aligned} \pi(m) + 1 > n &\Rightarrow 0 < \frac{n}{\pi(m) + 1} < 1 \\ &\Rightarrow \left[\frac{n}{\pi(m) + 1} \right] = 0 \end{aligned}$$

$$\Rightarrow \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} = 0$$

$$\Rightarrow \left[\left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} \right] = 0$$

On vient donc de montrer, dans les questions 4. a et 4. b, que : $\left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}} = \begin{cases} 1 & \text{si } \pi(m) \leq n - 1 \\ 0 & \text{sinon} \end{cases}$

5. Fixons un entier $n \geq 1$. On sait, d'après la première question, que $p_n \leq 2^n$. Ainsi, lorsque m varie entre 2 et 2^n , on a $\pi(m) \leq n - 1$ pour $2 \leq m \leq p_n - 1$, donc pour $p_n - 2$ valeurs.

Soit S la somme définie par :

$$S = \sum_{m=2}^{2^n} \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}}$$

Ce qui précède montre que dans cette somme, on fait la somme de 1 et de 0 et les chiffres 1 apparaissent $p_n - 2$ fois. On a donc

$$p_n - 2 = \sum_{m=2}^{2^n} \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}}$$

C'est - à - dire: $p_n = 2 + \sum_{m=2}^{2^n} \left[\frac{n}{\pi(m) + 1} \right]^{\frac{1}{n}}$

Soit enfin : $p_n = 2 + \sum_{m=2}^{2^n} \left[\frac{n}{1 + \sum_{j=2}^m \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right]} \right]^{\frac{1}{n}}$ *cqfd.*

Exercice 115[⊗]

On commence à vieillir quand on finit d'apprendre.

Complexité de l'algorithme d'Euclide

On se donne deux entiers strictement positifs a et b ($a \geq b$).

La recherche du PGCD de ces deux nombres à l'aide de l'algorithme d'Euclide se fait par divisions euclidiennes successives. Par exemple : $\text{PGCD}(48, 18) = 6$ car, successivement :

$$48 = 2 \times 18 + 12$$

$$18 = 1 \times 12 + 6$$

$$12 = 2 \times 6 + 0$$

Il a fallu trois divisions euclidiennes pour arriver à la conclusion. Mais plus généralement, combien faut-il de divisions pour arriver à obtenir le PGCD ?

Le théorème de Lamé donne une réponse à cette question. Il a pour énoncé :



"Le nombre de divisions euclidiennes nécessaires pour obtenir le PGCD de deux entiers naturels non nuls, en appliquant l'algorithme d'Euclide, est inférieur ou égal à 5 fois le nombre de chiffres servant à écrire le plus petit des deux nombres".

« Gabriel Lamé (1795-1870): physicien, mathématicien et ingénieur français. Il fut professeur de physique à l'école polytechnique de Paris, on lui doit des leçons sur les coordonnées curvilignes (appelées parfois coefficients de Lamé) et leurs applications ».

L'objectif du problème est de démontrer ce théorème.

Dans la suite, on désignera par $L(a, b)$ ce nombre de divisions nécessaires pour obtenir le PGCD de a et de b , en considérant que l'on s'arrête lorsqu'il apparaît un reste nul (le PGCD étant le dernier reste non nul). Ce nombre est la « longueur » de l'algorithme d'Euclide, pour les entiers a et b .

Partie A : Préliminaires

- Déterminer à titre d'exemple $L(585, 117)$ et $L(55, 34)$.
- Exploiter le 2^{ème} exemple étudié pour proposer des couples (a, b) d'entiers naturels tels que :
 - Le plus petit des entiers s'écrit avec un seul chiffre et $L(a, b) = 5$.
 - Le plus petit des entiers s'écrit avec deux chiffres, et $L(a, b) = 10$ (continuez la suite de « vers le haut »).

Partie B

Posons $d = \text{PGCD}(a, b) = a \wedge b$. Soit (F_n) la suite de Fibonacci définie par :

$$\begin{cases} F_1 = F_2 = 1 \\ F_{n+2} = F_{n+1} + F_n, \quad \forall n \geq 1 \end{cases}$$

Étude de quelques propriétés de (F_n)

- Montrer que la suite (F_n) est positive et strictement croissante à partir du rang 2.
- Donner le quotient et le reste de la division euclidienne de F_{n+2} par F_{n+1} .
- Que vaut $F_{n+2} \wedge F_{n+1}$? Combien de divisions ont été nécessaires pour la détermination de $F_{n+2} \wedge F_{n+1}$?
- On pose $\varphi = \frac{1+\sqrt{5}}{2}$ (nombre d'or).
 - Montrer que $\varphi^2 = \varphi + 1$ et plus généralement $\varphi^n = \varphi F_n + F_{n-1}$, $\forall n \geq 2$.
 - Montrer par récurrence sur n que $F_{n+2} \geq \varphi^n$, $\forall n \geq 1$.
- Notons n le nombre d'étapes nécessaires pour déterminer $a \wedge b$ grâce à l'algorithme d'Euclide (c'est-à-dire que $n = L(a, b)$). En posant $a = r_0$ et $b = r_1$, on peut écrire les divisions euclidiennes successives :

$$\begin{cases} r_0 = r_1 q_1 + r_2 \\ r_1 = r_2 q_2 + r_3 \\ \dots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n-1} = r_n q_n \end{cases}$$

- Montrer que si $q_n = 1$ alors $a \wedge b$ s'obtiendrait en $(n-1)$ étapes.
- En déduire que $r_{n-1} \geq F_3$.
- Établir par récurrence que $r_{n-k} \geq F_{k+2}$ pour tout $k \in \llbracket 1, n \rrbracket$.

Partie C : Démonstration du théorème de Lamé

- Montrer que $b \geq \varphi^{n-1}$.
 - En déduire que $\ln(b) \geq (n-1) \times \ln(\varphi)$.
2. Soit p le nombre de chiffres dans l'écriture de b en base 10.
- Justifier que $10^p > b$ puis en déduire que $p \times \ln(10) > (n-1) \times \ln(\varphi)$.
 - En admettant que $\ln(\varphi) \geq \frac{\ln(10)}{5}$ (on pourra le vérifier à la calculatrice), établir que $n \leq 5p$.

Corrigé

Partie A : Préliminaires

1. on a :

$$\rightarrow 585 = 117 \times 5 \text{ donc } L(585, 117) = 1.$$

$$\rightarrow 55 = 34 \times 1 + 21$$

$$34 = 21 \times 1 + 13$$

$$21 = 13 \times 1 + 8$$

$$13 = 8 \times 1 + 5$$

$$8 = 5 \times 1 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

$$\text{Donc } L(55, 34) = 8.$$

2.a. Pour avoir deux entiers naturels a et b tel que le plus petit b s'écrit avec un seul chiffre et $L(a, b) = 5$, il suffit de « gommer » les trois premières divisions dans le 2^{ème} exemple de la 1^{ère} question. Donc, on voit que les entiers $a = 13$ et $b = 8$ conviennent.

b. Il suffit de pousser les divisions de deux divisions vers le haut. Dans la 1^{ère} division additionnelle, le diviseur est 55, le quotient est 1 et le reste est 34 et donc le dividende est égal à $55 + 34 = 89$. Suivant le même principe, on trouve le dividende $89 + 55 = 144$ et le reste 89. Donc les entiers 144 et 89 conviennent.

Partie B : Étude de quelques propriétés de (F_n)

1. Soit la propriété (P_n) : « pour tout $n \geq 2$, $0 < F_n < F_{n+1}$ ».

Démontrons la propriété (P_n) par récurrence :

→ Initialisation : on a $F_3 = F_2 + F_1 = 1 + 1 = 2$.

Donc $0 < F_2 < F_3$ et la propriété est vraie pour $n = 2$.

→ Hérédité : On suppose qu'il existe un rang $n \geq 2$ pour lequel (P_n) est vraie c'est-à-dire que $0 < F_n < F_{n+1}$. Montrons que la propriété est vraie pour $n + 1$ c'est-à-dire que : $0 < F_{n+1} < F_{n+2}$

On sait que $F_{n+2} = F_{n+1} + F_n$.

Comme $0 < F_n$, alors $F_{n+1} + F_n > F_{n+1}$ et par suite $F_{n+2} > F_{n+1}$. Donc enfin : $0 < F_{n+1} < F_{n+2}$

D'autre part, on sait que $F_1 = 1 > 0$.

Donc en conclusion : $F_1 > 0$ et pour tout $n \geq 2$, $0 < F_n < F_{n+1}$.

La suite est à termes positifs et strictement croissante à partir du rang 2.

2. L'égalité $F_{n+2} = F_{n+1} + F_n$, avec $0 < F_n < F_{n+1}$ car la suite (F_n) est strictement croissante à partir de $n \geq 2$, traduit la division euclidienne de F_{n+2} par F_{n+1} . Donc le reste est égal à F_n .

3. Les égalités successives :

$$\begin{cases} F_{n+2} = F_{n+1} + F_n \\ F_{n+1} = F_n + F_{n-1} \\ \dots \\ F_3 = F_2 + F_1 \\ F_2 = F_1 + 0 \end{cases}$$

qui sont toutes des divisions euclidiennes montrent que $F_{n+2} \wedge F_{n+1} = 1$. Il a donc fallu $n - 1$ divisions euclidiennes sans compter bien sûr la dernière pour déterminer $F_{n+2} \wedge F_{n+1}$.

4. Soit $\varphi = \frac{1+\sqrt{5}}{2}$.

a. * Avec $\varphi = \frac{1+\sqrt{5}}{2}$, on vérifie tout banalement que $\varphi^2 = \varphi + 1$.

** Soit la propriété (Q_n) : « Pour tout $n \geq 2$, $\varphi^n = F_n \varphi + F_{n-1}$ ».

→ Initialisation :

On a $\varphi^2 = \varphi + 1 = \varphi F_2 + F_1$ car $F_2 = F_1 = 1$ et donc la propriété est vraie pour $n = 2$.

→ Hérédité :

On suppose que la propriété est vraie pour un rang donné $n \geq 2$, c'est-à-dire que :

$\varphi^n = F_n \varphi + F_{n-1}$, et montrons qu'elle l'est pour le rang $n + 1$ soit $\varphi^{n+1} = F_{n+1} \varphi + F_n$.

On sait que $\varphi^2 = \varphi + 1$ et $F_{n+1} = F_n + F_{n-1}$. D'où :

$$\begin{aligned} \varphi^{n+1} &= \varphi^n \times \varphi = (F_n \varphi + F_{n-1}) \times \varphi = F_n \varphi^2 + F_{n-1} \varphi = F_n(\varphi + 1) + F_{n-1} \varphi \\ &= (F_n + F_{n-1}) \varphi + F_n = F_{n+1} \varphi + F_n \quad \text{cqfd.} \end{aligned}$$

Donc la propriété (Q_n) est vraie pour tout $n \geq 2$.

b. On sait que $\varphi^n = F_n \varphi + F_{n-1}$ et que $\varphi \cong 1,618 < 2$, d'où :

$$\varphi^n = F_n \varphi + F_{n-1} < 2F_n + F_{n-1} = (F_n + F_{n-1}) + F_{n-1} < F_{n+1} + F_{n-1} < F_{n+1} + F_n = F_{n+2}.$$

Donc on a bien $F_{n+2} \geq \varphi^n$, $\forall n \geq 1$.

5.a. On remarque tout naturellement que $r_n \geq 1$.

Donc si l'on suppose que $q_n = 1$ alors on aurait $r_n = r_{n-1} = a \wedge b$ et par suite $a \wedge b$ s'obtiendrait en $(n - 1)$ étapes (divisions). Ce qui contredit l'hypothèse de n étapes nécessaires pour l'obtention de $a \wedge b$. En conclusion, q_n étant un entier distinct de 1 alors $q_n \geq 2$.

b. La dernière division dans la palette des divisions euclidiennes données, on a $r_{n-1} = r_n \times q_n$, et comme $r_n \geq 1$ et $q_n \geq 2$ alors $r_{n-1} = r_n \times q_n \geq 1 \times 2 = F_3$.

c. On a obtenu $r_{n-1} \geq F_3$ (donc la propriété est vraie pour $k = 1$).

Supposons que l'inégalité $r_{n-k} \geq F_{2+k}$ est vraie pour tout k compris entre 2 et $n - 1$. Montrons qu'elle est encore vraie pour n c'est-à-dire que $r_0 \geq F_{n+2}$.

On rappelle que :
$$\begin{cases} r_0 = r_1 q_1 + r_2 \\ r_1 = r_2 q_2 + r_3 \\ \dots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \\ r_{n-1} = r_n q_n \end{cases}$$

D'après l'hypothèse de récurrence :

$$r_1 = r_{n-(n-1)} \geq F_{2+(n-1)} = F_{n+1} \text{ et } r_2 = r_{n-(n-2)} \geq F_{2+(n-2)} = F_n$$

en outre $q_1 \geq 1$ et donc :

$$r_0 = r_1 q_1 + r_2 \geq r_1 + r_2 \geq F_{n+1} + F_n = F_{n+2}$$

Partie C : Démonstration du théorème de Lamé

1.a. En appliquant les résultats de la question 5.c. pour $k = n - 1$, on obtient $r_1 \geq F_{n+1}$ soit encore l'inégalité $b \geq F_{n+1}$ car $r_1 = b$. D'où enfin $b \geq F_{n+1} \geq \varphi^{n-1}$. Cqfd

b. La fonction $x \mapsto \ln(x)$ étant croissante sur $]0, +\infty[$, on déduit de l'inégalité $b \geq \varphi^{n-1}$ que :

$$\ln(b) \geq \ln(\varphi^{n-1}) = (n-1) \ln(\varphi)$$

2.a. Si p désigne le nombre de chiffres de b alors 10^p est le plus petit entier naturel qui s'écrit à l'aide de $p + 1$ chiffres et par conséquent $10^p > b$. On en déduit que $10^p > \varphi^{n-1}$ et via la fonction $\ln$, on conclut par le résultat : $p \times \ln(10) > (n-1) \ln(\varphi)$.

b. En tenant compte de $\ln(\varphi) \geq \frac{\ln(10)}{5}$ dans l'inégalité $p \times \ln(10) > (n-1) \ln(\varphi)$, on obtient :

$$p \times \ln(10) > (n-1) \ln(\varphi) \geq (n-1) \times \frac{\ln(10)}{5}$$

Soit : $p > \frac{n-1}{5}$ et vu que n est un entier $n \leq 5p$.

Conclusion : le nombre de divisions euclidiennes nécessaires pour déterminer le PGCD de a et b , en appliquant l'algorithme d'Euclide, est inférieur ou égal à 5 fois le nombre de chiffres servant à écrire le plus petit des deux nombres.



EXERCICES PROPOSES

Même un fusil maladroit atteindra la cible en multipliant les tirs.

Proverbe japonais

Exercice 1

Un nombre de quatre chiffres est un carré parfait. Le chiffre des unités est égal au chiffre des dizaines et le chiffre des centaines est égal au chiffre des unités de mille.

1. Montrer que ce nombre est divisible par 121. Trouver ce nombre.
2. Écrire ce nombre dans le système à base 8.

Exercice 2

Soit $n = \overline{cdu}$ un entier de trois chiffres divisible par 107.

Démontrer que l'entier naturel $x = 7d^2 + (7c - u)^2$ est aussi un multiple de 107.

☞ Lister tous les multiples de 107 de trois chiffres.

Exercice 3

On considère la suite (u_n) définie par $u_n = (3n - 1)^2 - 2 + (-2)^n$.

1. Démontrer que pour tout entier naturel n , $u_{n+1} + 2u_n$ est un multiple de 27.
2. Démontrer que tous les termes de la suite sont des multiples de 27.

Exercice 4

Soit n un entier naturel supérieur ou égal à 1.

1. Démontrer que $9^{n+1} - 2^{n+1} = 11(9^n - 2^n) - 18(9^{n-1} - 2^{n-1})$.
2. Démontrer, par récurrence, que $3^{2n} - 2^n$ est divisible par 7.

Exercice 5

1. Démontrer que le nombre $A = a(a^2 - 1)$ est divisible par 6.

2. Plus généralement, démontrer que $A_n = a(a^{2n} - 1)$ est divisible par 6 (n désigne un entier naturel quelconque).

Application : Démontrer que les sommes : $S = a_1 + a_2 + \dots + a_k$ et $S_n = a_1^{2n+1} + a_2^{2n+1} + \dots + a_k^{2n+1}$ dans lesquelles $a_1, a_2, \dots, a_k$ désignent des entiers naturels non nuls donnés, ont le même reste dans la division euclidienne par 6.

Exercice 6

1. Vérifier que, pour tout entier naturel n , on a : $7^{3n} \equiv 1 [19]$. En déduire que, quels que soient les naturels n et k , on peut écrire : $7^{3n+k} \equiv 7^k [19]$. Quels sont les restes possibles dans la division euclidienne de 7^n par 19 ?

2. Démontrer que pour trois entiers naturels consécutifs a, b et c , l'entiers $7^a + 7^b + 7^c$ est un multiple de 19.

Exercice 7

1. Déterminer, suivant le reste de la division euclidienne de n par 7, celui de la division euclidienne de n^3 par 7.

2. Démontrer que si $a^3 + b^3 + c^3 \equiv 0 [7]$, alors : $abc \equiv 0 [7]$.

Exercice 8

1. Soit x un entier relatif. En discutant suivant les valeurs de x modulo 9, déterminer le reste de la division euclidienne de x^3 par 9. En déduire que, pour tout entier relatif x , on a :

$$x^3 \equiv 0 [9] \Leftrightarrow x \equiv 0 [3], \quad x^3 \equiv 1 [9] \Leftrightarrow x \equiv 1 [3], \quad x^3 \equiv 8 [9] \Leftrightarrow x \equiv 2 [3]$$

2. On considère trois entiers relatifs x, y et z tels que $x^3 + y^3 + z^3$ soit divisible par 9.

Démontrer que l'un des trois entiers x, y ou z est divisible par 3.

Exercice 9

Le but de l'exercice est de montrer que, pour tout entiers naturel n , on ne peut pas écrire $2^n + 1$ sous la forme p^3 avec p un nombre premier supérieur à 3. Pour cela, on suppose par l'absurde qu'il existe un entiers naturel premier p supérieur à 3 tel que $2^n + 1 = p^3$.

- 1.a. Montrer que si n est impair alors $2^n + 1 \equiv 0 \pmod{3}$.
- b. Dédurre que $p = 3$ puis conclure.
2. On suppose que n est pair. On écrit $n = 2k$ avec $k \in \mathbb{N}$.
 - Le cas où k est impair (on dit que n est impairement pair).
 - a. Montrer que si k est impair alors $2^n + 1 \equiv 0 \pmod{5}$.
 - b. Dédurre que si k est impair alors $p = 5$.
 - c. Montrer que si k est impair alors 31 divise 2^n . Conclure.
 - Le cas où k est pair (on dit que n est pairement pair).
 - a. Déterminer dans ce cas les restes possibles de $2^n + 1$ modulo 7.
 - b. Pour un entier m , quels sont les restes possibles de m^3 modulo 7.
 - c. Conclure.

Exercice 10

Le produit de deux entiers naturels a et b ($a < b$) est 11 340. On note d leur PGCD.

- 1.a. Pourquoi d^2 divise-t-il 11 340 ?
- b. Pourquoi $d = 2^\alpha \times 3^\beta$ avec $0 \leq \alpha \leq 1$ et $0 \leq \beta \leq 2$?
2. On sait de plus que a et b ont six diviseurs communs et que l'entier a est un multiple de 5.
 - a. Démontrer que $d = 18$.
 - b. En déduire a et b .

Exercice 11

α et β sont deux naturels et $n = 2^\alpha \times 3^\beta$.

Le nombre de diviseurs de n^2 est le triple du nombre de diviseurs de n .

1. Prouver que $(\alpha - 1)(\beta - 1) = 3$.
2. En déduire n .

Exercice 12

Question de cours

On rappelle la propriété :

Si $a \equiv b \pmod{n}$ alors, pour tout $c \in \mathbb{Z}$, $ac \equiv bc \pmod{n}$.

En utilisant cette propriété, démontrer par récurrence: Si $a \equiv b \pmod{n}$ alors, pour tout $k \in \mathbb{Z}$, $a^k \equiv b^k \pmod{n}$.

1. Compléter le tableau :

$n \equiv \dots \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$3^n \equiv \dots \pmod{10}$										

2. Montrer que si $n \equiv 0 \pmod{4}$ alors $3^n \equiv 1 \pmod{10}$.
3. Qu'en est-il si $n \equiv 2 \pmod{4}$?
4. Déterminer le chiffre des unités de 2013^{20214} .
5. Démontrer que $3^{2013} + 3^{2015}$ est divisible par 10.

Exercice 13

Soit A l'ensemble des entiers naturels de l'intervalle $[1; 46]$.

1. On considère l'équation (E) : $23x + 47y = 1$ où x et y sont des entiers relatifs.

- a. Donner une solution particulière (x_0, y_0) de (E).
- b. Déterminer l'ensemble des couples (x, y) solutions de (E).
- c. En déduire qu'il existe un unique entier x de A tel que $23x \equiv 1 \pmod{47}$.

2. Soient a et b deux entiers relatifs.

- a. Montrer que si $ab \equiv 0 \pmod{47}$ alors $a \equiv 0 \pmod{47}$ ou $b \equiv 0 \pmod{47}$.
- b. En déduire que si $a^2 \equiv 1 \pmod{47}$ alors $a \equiv 1 \pmod{47}$ ou $a \equiv -1 \pmod{47}$.
3. a. Montrer que pour tout entier p de A , il existe un entier relatif q tel que $p \times q \equiv 1 \pmod{47}$.

Pour la suite, on admet que pour tout entier p de A , il existe un unique entier, noté $\text{inv}(p)$, appartenant à A tel que $p \times \text{inv}(p) \equiv 1 \pmod{47}$. Par exemple : $\text{inv}(1) = 1$ car $1 \times 1 \equiv 1 \pmod{47}$, $\text{inv}(2) = 24$ car $2 \times 24 \equiv 1 \pmod{47}$, $\text{inv}(3) = 16$ car $3 \times 16 \equiv 1 \pmod{47}$.

- b. Quels sont les entiers p de A qui vérifient $p = \text{inv}(p)$?
- c. Montrer que $46! \equiv -1 \pmod{47}$.

Exercice 14

On rappelle la propriété connue sous le nom du petit théorème de Fermat:

« Si p est un nombre premier et q un entier naturel premier avec p , alors on a $q^{p-1} \equiv 1 \pmod{p}$ ».

On considère la suite (un) définie pour tout entier naturel n non nul par : $u_n = 2^n + 3^n + 6n - 1$.

1. Calculer les six premiers termes de la suite.
2. Montrer que, pour tout entier naturel n non nul, u_n est pair.

3. Montrer que, pour tout entier naturel n pair non nul, u_n est divisible par 4.
On note (E) l'ensemble des nombres premiers qui divisent au moins un terme de la suite (u_n) .
4. Les entiers 2, 3, 5 et 7 appartiennent-ils à l'ensemble (E) ?
5. Soit p un nombre premier strictement supérieur à 3.
 - a. Montrer que: $6 \times 2p - 2 \equiv 3 [p]$ et $6 \times 3p - 2 \equiv 2 [p]$.
 - b. En déduire que $6u_p - 2 \equiv 0 [p]$.
 - c. Le nombre p appartient-il à l'ensemble (E) ?

Exercice 15

1. a. Pour $1 \leq n \leq 6$, calculer les restes de la division euclidienne de 3^n par 7.
- b. Démontrer que, pour tout n , $3^{n+6} - 3^n$ est divisible par 7. En déduire que 3^{n+6} et 3^n ont même reste dans la division par 7.
- c. A l'aide des résultats précédents, calculer le reste de la division euclidienne de 3^{1000} par 7.
- d. De manière générale, comment peut-on calculer le reste de la division euclidienne de 3^n par 7, pour n quelconque ?
- e. En déduire que, pour tout entier naturel n , 3^n est premier avec 7.
2. Soit la somme : $u_n = 1 + 3 + 3^2 + \dots + 3^{n-1} = \sum_{i=0}^{n-1} 3^i$ pour n entier supérieur ou égal à 2.
 - a. Montrer que $u_n = \frac{1}{2}(3^n - 1)$.
 - b. Déterminer les valeurs de n telles que u_n soit divisible par 7.
 - c. Déterminer tous les diviseurs de u_6 .

Exercice 16

p est un nombre premier différent de 2.

1. Dresser la liste des diviseurs de p^4 ? On appelle S la somme de ses diviseurs.
2. Démontrer que quelque soit p , on a : $(2p^2 + p)^2 < S < (2p^2 + p + 2)^2$.
3. On cherche maintenant à déterminer p pour que S soit un carré parfait (c'est-à-dire le carré d'un entier n).
 - a. Démontrer que $2p^2 + p < 2n < 2p^2 + p + 2$.
 - b. Exprimer alors n en fonction de p .
 - c. Déterminer les couples (n, p) qui répondent à la question.

Exercice 17

n est un entier $n \geq 1$, $a = n^{13} - n$.

1. Prouver que a est pair.
2. Prouver que a est divisible par 13 et par 7.
3. En déduire que a est divisible par 182.

Exercice 18 (Le PPND)

Soit n est un entier naturel non nul. On définit $\Delta(n)$ comme étant le **Plus Petit Non-Diviseur** de n , c'est-à-dire le plus petit entier strictement positif qui ne divise pas n .

1. Déterminer $\Delta(2)$, $\Delta(6)$, $\Delta(153)$. Peut-on trouver n tel que $\Delta(n) = 1$?
2. Soit n impair. Que vaut $\Delta(n)$?
3. Montrer que si n divise m alors $\Delta(n)$ divise $\Delta(m)$.
 - a. Soit n et p tels que $\Delta(n) = p$ avec p premier, et soit m non divisible par p . Que vaut $\Delta(mn)$?
 - b. En déduire qu'il y a une infinité d'entiers tels que $\Delta(n) = p$.
4. Soit p premier.
 - a. Déterminer $\Delta((p-1)!)$.
 - b. En déduire que pour tout p premier, il existe n tel que $\Delta(n) = p$.
5. Est-il possible de trouver n tel que $\Delta(n) = 6$? Expliquer.
6. Montrer que $\Delta(n)$ est soit un nombre premier, soit la puissance d'un nombre premier.
7. Soit p premier et k un entier naturel non nul. Trouver n tel que $\Delta(n) = p^k$.

Exercice 19

Dans le plan muni d'un repère orthonormé $(O; \vec{u}, \vec{v})$, on donne le point A de coordonnées $(12; 18)$.

On désigne par B un point de l'axe $(O; \vec{u})$ et par C un point de l'axe $(O; \vec{v})$ tels que : $(\vec{AB}, \vec{AC}) = -\frac{\pi}{2}$

On appelle x l'abscisse de B et y l'ordonnée de C .

1. Démontrer que le couple $(x; y)$ est solution de l'équation $(E) : 2x + 3y = 78$.
2. On se propose de trouver tous les couples (B, C) de points ayant pour coordonnées des nombres entiers relatifs.

- a) Montrer que l'on est ramené à l'équation (E), avec x et y appartenant à l'ensemble $\mathbb{Z}$ des nombres entiers relatifs.
- b) À partir de la définition de B et C , trouver une solution particulière $(x_0; y_0)$ de (E) avec x_0 et y_0 appartenant à l'ensemble $\mathbb{Z}$.
- c) Démontrer qu'un couple $(x; y)$ d'entiers relatifs est solution de l'équation (E) si, et seulement si, il est de la forme : $(12 + 3k; 18 - 2k)$, où k appartient à $\mathbb{Z}$.
- d) Combien y a-t-il de couples de points (B, C) ayant pour coordonnées des nombres entiers relatifs, tels que :
 $-6 \leq x \leq 21$ et $-5 \leq y \leq 14$?

Exercice 20

1. Le plan (P) est rapporté à un repère orthonormé direct $(O; \vec{u}, \vec{v})$.

Soit A et B dans ce plan d'affixes respectives $a = 1 + i$; $b = -4 - i$.

Soit f la transformation du plan (P) qui à tout point M d'affixe z associe le point M' d'affixe z' tel que :

$$\overrightarrow{OM'} = 2\overrightarrow{AM} + \overrightarrow{BM}.$$

a. Exprimer z' en fonction de z .

b. Montrer que f admet un seul point invariant Ω dont on donnera l'affixe. En déduire que f est une homothétie dont on précisera le centre et le rapport.

2. On se place dans le cas où les coordonnées x et y du point M sont des entiers avec $1 \leq x \leq 8$ et $1 \leq y \leq 8$.

Les coordonnées $(x'; y')$ de M' sont alors : $x' = 3x + 2$ et $y' = 3y - 1$.

a. On appelle G et H les ensembles des valeurs prises respectivement par x' et y' . Écrire la liste des éléments des ensembles G et H .

b. Montrer que $x' - y'$ est un multiple de 3.

c. Montrer que la somme et la différence de deux entiers quelconques ont même parité. On se propose de déterminer tous les couples $(x'; y')$ de $G \times H$ tels que $m = x'^2 - y'^2$ soit un multiple non nul de 60.

d. Montrer que dans ces conditions, $x' - y'$ est un multiple de 6. Le nombre $x' - y'$ peut-il être un multiple de 30 ?

e. En déduire que, si $x'^2 - y'^2$ est un multiple non nul de 60, $x' + y'$ est multiple de 10 et utiliser cette condition pour trouver tous les couples $(x'; y')$ qui conviennent. En déduire les couples $(x; y)$ correspondant aux couples $(x'; y')$ trouvés.

Exercice 21

Les trois questions de cet exercice sont indépendantes.

1. a. Déterminer l'ensemble des couples (x, y) de nombres entiers relatifs, solution de l'équation (E) : $8x - 5y = 3$.

b. Soit m un nombre entier relatif tel qu'il existe un couple (p, q) de nombres entiers vérifiant : $m = 8p + 1$ et $m = 5q + 4$.

Montrer que le couple (p, q) est solution de l'équation (E) et en déduire la congruence $m \equiv 9 \pmod{40}$.

c. Déterminer le plus petit de ces nombres entiers m supérieurs à 2 000.

2. Soit n un nombre entier naturel.

a. Démontrer que pour tout nombre entier naturel k on a : $23k \equiv 1 \pmod{7}$.

Quel est le reste dans la division euclidienne de 22009 par 7 ?

3. Soient a et b deux nombres entiers naturels inférieurs ou égaux à 9 avec la condition $a \neq 0$.

On considère le nombre $N = a \times 103 + b$. On rappelle qu'en base 10 ce nombre s'écrit sous la forme $N = \overline{a00b}$.

On se propose de déterminer parmi ces nombres entiers naturels N ceux qui sont divisibles par 7.

a. Vérifier que $103 \equiv -1 \pmod{7}$.

b. En déduire tous les nombres entiers N cherchés.

Exercice 22

Dans cette partie, on se propose d'étudier des couples (a, b) d'entiers strictement positifs, tels que : $a^2 = b^3$

Soit (a, b) un tel couple et $d = \text{PGCD}(a, b)$. On note u et v les entiers tels que : $a = du$ et $b = dv$.

1. Montrer que $u^2 = dv^3$.

2. En déduire que v divise u , puis que $v = 1$.

3. Soit (a, b) un couple d'entiers strictement positifs. Démontrer que l'on a $a^2 = b^3$ si et seulement si a et b sont respectivement le cube et le carré d'un même entier.

4. Montrer que si n est le carré d'un nombre entier naturel et le cube d'un autre entier, alors : $n \equiv 0 \pmod{7}$ ou $n \equiv 1 \pmod{7}$.

Exercice 23

Partie A : On admet que 1999 est un nombre premier. Déterminer l'ensemble des couples $(a; b)$ d'entiers naturels admettant pour somme 11 994 et pour PGCD 1999.

Partie B : On considère l'équation (E) d'inconnue n appartenant à $\mathbb{N}$: $(E) : n^2 - Sn + 11994 = 0$ où S est un naturel. On s'intéresse à des valeurs de S telles que (E) admette deux solutions dans $\mathbb{N}$.

1. Peut-on déterminer un entier S tel que 3 soit solution de (E) ? Si oui, préciser la deuxième solution.
2. Peut-on déterminer un entier S tel que 5 soit solution de (E) ?
3. Montrer que tout entier n solution de (E) est un diviseur de 11994. En déduire toutes les valeurs possibles de S telles que (E) admette deux solutions entières.

Partie C : Comment montrerait-on que 1999 est un nombre premier ? Préciser le raisonnement employé.

La liste de tous les entiers premiers inférieurs à 100 est précisée ci-dessous :

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.

Exercice 24

Partie A : Question de cours

Quelles sont les propriétés de compatibilité de la relation de congruence avec l'addition, la multiplication et les puissances ?

Démontrer la propriété de compatibilité avec la multiplication.

Partie B : On note 0, 1, 2, ..., 9, α , β les chiffres de l'écriture d'un nombre en base 12. Par exemple :

$$\overline{\beta\alpha 7}^{12} = \beta \times 12^2 + \alpha \times 12 + 7 = 11 \times 144 + 10 \times 12 + 7 = 1711 \text{ en base 10.}$$

1. a. Soit N_1 le nombre s'écrivant en base 12 : $N_1 = \overline{\beta 1 \alpha}^{12}$. Déterminer l'écriture de N_1 en base 10.

b. Soit N_2 le nombre s'écrivant en base 10 : $N_2 = 1131 = 1 \times 10^3 + 1 \times 10^2 + 3 \times 10 + 1$.

Déterminer l'écriture de N_2 en base 12.

Dans toute la suite un entier naturel N s'écrit de manière générale en base 12 : $N = \overline{a_n a_{n-1} \dots a_1 a_0}^{12}$

2. a. Démontrer que $N \equiv a_0 [3]$. En déduire un critère de divisibilité par 3 d'un nombre écrit en base 12.

b. À l'aide de son écriture en base 12, déterminer si N_2 est divisible par 3. Confirmer avec son écriture en base 10.

3. a. Démontrer que $N \equiv a_n + a_{n-1} + \dots + a_1 + a_0 [11]$.

En déduire un critère de divisibilité par 11 d'un nombre écrit en base 12.

b. À l'aide de son écriture en base 12, déterminer si N_1 est divisible par 11.

Confirmer avec son écriture en base 10.

4. Un nombre N s'écrit $N = \overline{x4y}^{12}$. Déterminer les valeurs de x et de y pour lesquelles N est divisible par l'entier 33.

Exercice 25 (Système bibinaire)



Boby Lapointe, de son vrai nom **Robert Jean-François Joseph Pascal Lapointe**, (1922-1972) était un poète-fantaisiste-auteur-compositeur-interprète...

Il avait aussi une solide formation mathématique et on ne peut pas résister au plaisir de présenter dans cet exercice le système de numération qu'il a imaginé. Il s'agit du **SYSTEME BIBINAIRE** qui lui valut un succès et une estime auprès de la communauté scientifique en 1971. Comme beaucoup de réformateurs des systèmes de numération, Mr. Bobby Lapointe rejette le système décimal actuel notamment à cause des expressions du genre soixante-seize ou quatre-vingt-dix-sept.

Il est amusant de noter que le langage inventé par Bobby fait appel aux deux codages de base utilisés en informatique :

→ Le système binaire, envisagé par Neper en 1616 et popularisé par Leibniz au 18^{ème} siècle, qui n'utilise que les deux chiffres 0 et 1.

→ Le système hexadécimal, dont les seize chiffres sont notés 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F.

Examinons le système **BIBI**. Ils existent le **BIBI** parlé et le **BIBI** écrit que quelques exemples vont vous faire découvrir : Les naturels de zéro à quinze sont écrits dans le système binaire, en rajoutant éventuellement des zéros au début pour avoir quatre chiffres :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
000	000	001	001	010	010	011	011	100	100	101	101	110	110	111	111
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Découpant l'écriture de ces naturels en tranches de deux chiffres, on obtient quatre groupements possibles :

00, 01, 10 et 11.

Pour les groupes de deux chiffres terminant l'écriture d'un naturel, on choisit quatre voyelles :

00 → O ; 01 → A ; 10 → E ; 11 → I et pour le premier groupe de deux chiffres, on choisit quatre consonnes : 00 → H ; 01 → B ; 10 → K ; 11 → D.

Utilisant ce code, voici l'écriture des seize premiers naturels :

HO	HA	HE	HI	BO	BA	BE	BI	KO	KA	KE	KI	DO	DA	DE	DI
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Notons au passage l'importance du "H" (muet) et des consonnes dures "B" et "K" ce qui va donner au BIBI parlé une note enfantine agréable à l'oreille ! Il reste à associer ces seize phonèmes afin de représenter les naturels supérieurs à quinze.

On considère alors une numération de base seize (système hexadécimal) et on obtient les exemples suivants:

$$31 = (1 \times 16) + 15 \rightarrow \text{HADI}$$

$$16 = (1 \times 16) + 0 \rightarrow \text{HAHO}$$

$$1000 = (3 \times 16 \times 16) + (14 \times 16) + 8 \rightarrow \text{HIDEKO}$$

1. Écrire en base dix les naturels suivants KADO, HABIHABOBO, KEKIDIBOBI...

2. Traduire en système BIBINAIRE : 680 et 2005.

3. Écrire et apprendre par cœur la table de multiplication par BA. Donnons le départ :

$$BA \text{ fois } HO \rightarrow HO; \quad BA \text{ fois } HA \rightarrow BA; \quad BA \text{ fois } HE \rightarrow KE; \quad \dots\dots$$

4. Enfin, Bobby Lapointe était aussi un affreux mais émérite auteur de calembours, et pour le savoir, effectuer les opérations suivantes : HABI fois HABI égale ... ; HABI plus HABI égale ...

Exercice 26

On considère le nombre A qui s'écrit dans le système décimal $A = \overline{xyxyxyxyx}5$, x et y étant des chiffres de ce système, x étant non nul.

1. A quelle condition, ce nombre est-il divisible par 25 ?

2. Déterminer les différentes valeurs de A , telles que A soit divisible par 225.

3. On considère le nombre $B = \overline{xyxyxy}$ toujours écrit dans le système décimal avec x et y des chiffres, x étant non nul. Déterminer B tel que B soit divisible par 225.

Exercice 27

Soit n un entier relatif quelconque. On pose $A = n - 1$ et $B = n^2 - 3n + 6$.

1. a. Montrer que le PGCD de A et B est égal au PGCD de A et 4.

b. Déterminer, suivant les valeurs de n , le PGCD de A et B .

2. Pour quelles valeurs de l'entier relatif $n \neq 1$, $\frac{n^2 - 3n + 6}{n - 1}$ est-il entier relatif ?

Exercice 28

1. Déterminer l'ensemble U des entiers relatifs n tels que $n + 2$ divise $2n + 1$.

2. Montrer que pour tout entier relatif, les nombres $n + 2$ et $2n^2 + 3n - 1$ sont premiers entre eux.

3. Déterminer l'ensemble V des entiers relatifs n , $n \neq -2$ tels que $\frac{(2n-1)(2n^2+3n-1)}{(n^2-2)(n+2)}$ soit un entier relatif.

Exercice 29

Le nombre n désigne un entier naturel.

1. Démontrer que $n^2 + 5n + 4$ et $n^2 + 3n + 2$ sont divisibles par $n + 1$.

2. Déterminer l'ensemble des valeurs de n pour lesquelles $3n^2 + 15n + 19$ est divisible par $n + 1$.

3. En déduire que, quel que soit n , $3n^2 + 15n + 19$ n'est pas divisible par $n^2 + 3n + 2$.

Exercice 30

Pour tout entier naturel n supérieur ou égal à 5, on considère les nombres : $a = n^3 - n^2 - 12n$ et $b = 2n^2 - 7n - 4$.

1. Montrer, après factorisation, que a et b sont des entiers naturels divisibles par l'entier $n - 4$.

2. On pose $\alpha = 2n + 1$ et $\beta = n + 3$. On note d le PGCD de α et β .

a. Établir une relation entre α et β indépendante de n .

b. Démontrer que d est un diviseur de 5.

c. Démontrer que les nombres α et β sont multiples de 5 si et seulement si l'entier $n - 2$ est multiple de 5.

3. Montrer que $2n + 1$ et n sont premiers entre eux.

4.a. Déterminer, suivant les valeurs de n et en fonction de n le PGCD de a et b .

b. Vérifier les résultats obtenus dans les cas particuliers $n = 11$ et $n = 12$.

Exercice 31

On note n un entier naturel non nul, A l'entier naturel $3n + 1$ et B l'entier naturel $5n - 1$.

1. Démontrer que le PGCD de A et B est un diviseur de 8.

2. Pour quelles valeurs de n ce PGCD est-il égal à 8 ? Calculer alors le PPCM de A et B .

3. Pour quelles valeurs de n ce PGCD est-il égal à 3 ?

Exercice 32

Soit a et b deux entiers naturels premiers entre eux.

1. Montrer que $a + b$ et ab sont premiers entre eux.

2.a. Vérifier que $a^2 - ab + b^2 = (a + b)^2 - 3ab$.

b. En déduire que $a + b$ et $a^2 - ab + b^2$ sont soit premiers entre eux, soit divisibles par 3.

3. Démontrer l'égalité : $\text{PGCD}(a + b, a^2 - ab + b^2) = \text{PGCD}(a + b, 3)$.

Exercice 33

1. Soit a et b deux entiers relatifs non nuls et k un entiers relatif tel que $a + kb > 0$.

Montrer que : $\text{PGCD}(a, b) = \text{PGCD}(a + kb, b)$.

Exemple : $\text{PGCD}(325, 70) = \text{PGCD}(325 - 4 \times 70, 70)$.

2. Déterminer, par ce procédé, le $\text{PGCD}(628, 103)$.

3. n étant un entier supérieur ou égal à 2, on pose : $a = n^2 - 4n$ et $b = 2n$.

Montrer que $\text{PGCD}(a, b) = n \times \text{PGCD}(n, 2)$. Étudier, suivant la parité de n , le PGCD de a et b .

Exercice 34

Soient m et n deux entiers naturels, avec $m < n$, et tels que $m^n = n^m$.

1. Vérifier que $m = 0$ et $m = 1$ ne donnent aucune solution.

2. Pour $m \geq 2$, montrer que : $m^n = n^m \Leftrightarrow f(m) = f(n)$ avec $f(x) = \frac{\ln x}{x}$

3. En étudiant les variations de la fonction $f : x \mapsto \frac{\ln x}{x}$ sur l'intervalle $[2; +\infty[$, déterminer les couples solutions (m, n) de l'identité $m^n = n^m$.

Exercice 35

1. Soit n un entier naturel.

a. Montrer que si n est impair alors : $n^2 \equiv 1 \pmod{8}$.

b. Montrer que si n est pair alors : $n^2 \equiv 0 \pmod{8}$ ou $n^2 \equiv 4 \pmod{8}$.

2. Les nombres a , b et c sont trois entiers naturels impairs.

a. Montrer que : $a^2 + b^2 + c^2$ n'est pas un carré parfait.

b. Montrer que : $2(ab + bc + ca) \equiv 6 \pmod{8}$. (On pourra développer $(a + b + c)^2$).

c. En déduire que $2(ab + bc + ca)$ n'est pas un carré parfait.

d. Montrer que $ab + bc + ca$ n'est pas un carré parfait.

Exercice 36

Pour tout entier n non nul, on considère les nombres : $a_n = 4 \times 10^n - 1$, $b_n = 2 \times 10^n - 1$, $c_n = 2 \times 10^n + 1$.

1.a) Calculer a_1 , b_1 , c_1 , a_2 , b_2 , c_2 , a_3 , b_3 et c_3 .

b) Combien les écritures décimales des nombres a_n et c_n ont-elles de chiffres ? Montrer que a_n et c_n sont divisibles par 3.

c) Montrer, en utilisant la liste des nombres premiers inférieurs à 100 donnée ci-dessous, que b_3 est premier.

d) Montrer que, pour tout entier naturel non nul n , $b_n \times c_n = a_{2n}$.

En déduire la décomposition en produit de facteurs premier de a_6 .

e) Montrer que $\text{PGCD}(b_n, c_n) = \text{PGCD}(c_n, 2)$. En déduire que b_n et c_n sont premiers entre eux.

2. On considère l'équation (1) : $b_3x + c_3y = 1$ dont les inconnues sont les entiers relatifs x et y .

a) Justifier le fait que (1) possède au moins une solution.

b) Appliquer l'algorithme d'Euclide aux nombres c_3 et b_3 ; en déduire une solution particulière de (1).

c) Résoudre l'équation (1).

LISTE DES NOMBRES PREMIERS INFÉRIEURS A 100 :

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.

Exercice 37

Le nombre n est un entier naturel non nul ; on pose $a = 4n + 3$ et $b = 5n + 2$ et on note d le PGCD de a et b .

1. Complétez le tableau ci-dessous. Quelle conjecture pouvez-vous faire sur d ?

n	a	b	d
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

2. Calculer $5a - 4b$ et en déduire les valeurs possibles de d .

3. On considère l'équation (E) : $7k - 4n = 3$, où n et k sont deux naturels non nuls.

a. Déterminer une solution particulière de (E), puis tous les couples solutions de (E).

b. En déduire tous les couples d'entiers naturels $(n; k)$ solutions du problème tels que $4n + 3 = 7k$.

4. Déterminer, à l'aide des congruences, les entiers naturels n tels que $5n + 2$ soit divisible par 7.

5. Soit r le reste de la division euclidienne de n par 7. Déduire des questions précédentes la valeur de r pour laquelle d vaut 7. Pour quelles valeurs de r , d est-il égal à 1 ?

Exercice 38

1. On considère l'équation (E) : $6x + 7y = 57$ où x et y sont des entiers relatifs.

a. Déterminer un couple de relatifs (u, v) tel que $6u + 7v = 1$; en déduire une solution (x_0, y_0) de (E).

b. Déterminer les couples d'entiers relatifs solutions de l'équation (E).

2. Soit $(O; \vec{i}, \vec{j}, \vec{k})$ un repère orthonormal de l'espace. On considère le plan P d'équation :

$6x + 7y + 8z = 57$ et on considère les points du plan P qui appartiennent aussi au plan $(O; \vec{i}, \vec{j})$. Montrer qu'un seul de ces points a pour coordonnées des entiers naturels que l'on déterminera.

3. On considère un point M du plan P dont les coordonnées x, y et z sont des entiers naturels.

a. Montrer que l'entier y est impair.

b. On pose $y = 2p + 1$ où p est un entier naturel.

Montrer que le reste dans la division euclidienne de $p + z$ par 3 est égal à 1.

c. On pose $p + z = 3q + 1$ où q est un entier naturel.

Montrer que les entiers naturels x, p et q vérifient la relation : $x + p + 4q = 7$

En déduire que q prend les valeurs 0 ou 1.

d. En déduire les coordonnées de tous les points de P dont les coordonnées sont des entiers naturels.

Exercice 39

Partie A : On rappelle ci-dessous le théorème de BÉZOUT et le théorème de GAUSS.

Théorème de BÉZOUT : Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe un couple (u, v) d'entiers relatifs vérifiant $au + bv = 1$.

Théorème de GAUSS : Soient a, b, c des entiers relatifs.

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

1. En utilisant le théorème de BÉZOUT, démontrer le théorème de GAUSS.

2. Soient p et q deux entiers naturels tels que p et q sont premiers entre eux.

Déduire du théorème de GAUSS que, si a est un entier relatif, tel que $a \equiv 0 [p]$ et $a \equiv 0 [q]$, alors on a : $a \equiv 0 [pq]$.

Partie B : On se propose de déterminer l'ensemble S des entiers relatifs n vérifiant le système : $\begin{cases} n \equiv 9 [17] \\ n \equiv 3 [5] \end{cases}$

1. Recherche d'un élément de S . On désigne par (u, v) un couple d'entiers relatifs tel que $17u + 5v = 1$.

a. Justifier l'existence d'un tel couple (u, v) .

b. On pose $n_0 = 3 \times 17u + 9 \times 5v$. Démontrer que n_0 appartient à S .

c. Donner un exemple d'entier n_0 appartenant à S .

2. Caractérisation des éléments de S .

a. Soit n un entier relatif appartenant à S . Démontrer que $n - n_0 \equiv 0 [85]$.

b. En déduire qu'un entier relatif n appartient à S si et seulement si n peut s'écrire sous la forme suivante $n = 43 + 85k$ où k est un entier relatif.

3. Application : Zeinebou sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9. Si elle fait des tas de 5 jetons, il lui en reste 3. Combien a-t-elle de jetons ?

Exercice 40

Soit la suite (U_n) définie sur $\mathbb{N}$ par :

$$\begin{cases} U_n = 0 \\ \forall n \in \mathbb{N}, U_{n+1} = \sqrt{pU_n^2 + 1} \end{cases}, \text{ où } p \text{ est un réel non nul.}$$

1. On suppose que $p = 1$.

Montrer que : $\forall n \in \mathbb{N}, U_n = \sqrt{n}$.

Calculer : $\lim_{n \rightarrow +\infty} U_n$.

2. On suppose que $p \in]0, 1[$.

a. Montrer que :

$$\forall n \in \mathbb{N}, 0 \leq U_n < \frac{1}{\sqrt{1-p}}$$

b. Étudier la monotonie de la suite (U_n) . En déduire que (U_n) est convergente et calculer sa limite.

3. On suppose que $p \in]1, +\infty[$.

On pose $S_n = 1 + p + p^2 + \dots + p^{n-1}$, pour $n \in \mathbb{N}^*$.

a. Montrer que : $\forall n \in \mathbb{N}, U_{n+1}^2 - U_n^2 = p^n$.

b. En déduire que : $\forall n \in \mathbb{N}^*, U_n = \sqrt{S_n}$.

4. On suppose que p est un entier différent de 1.

a. Calculer $p^n + (1-p)U_n^2$. En déduire que p^n et $1-p$ sont premiers entre eux.

b. Soit dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E_n) : $p^n x - (1-p)y = p$.

Justifier que l'équation (E_n) possède des solutions dans $\mathbb{Z} \times \mathbb{Z}$ et vérifier que les solutions de (E_n) sont les couples $(p + k(1 - p), -U_n^2 + kp^n)$, $k \in \mathbb{Z}$.

c. En déduire dans $\mathbb{Z} \times \mathbb{Z}$ les solutions de l'équation : $10^n x + 2^{n+2} y = 10 \times 2^{n-1}$.

Exercice 41

1.a. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(E) : 6X - 5Y = 7$.

b. Déterminer alors les solutions dans $\mathbb{N}$ du système suivant : $\begin{cases} n \equiv 2 \pmod{6} \\ n \equiv 9 \pmod{5} \end{cases}$.

c. Déterminer les solutions dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation : $(6X - 5Y - 6)(6X - 5Y + 6) = 13$.

2. On considère dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(E') : 6X^2 - 5Y^2 = 7$.

a. Montrer que si (X, Y) est une solution de (E') alors $X^2 \equiv 2 \pmod{5}$.

b. Quel est alors l'ensemble des solutions de (E') ?

3. On considère dans $\mathbb{Z}^3$ l'équation $(E'') : 6X - 5Y - 4Z = 7$.

a. Montrer que Y est impair.

b. On pose $Y = 2p + 1$; ($p \in \mathbb{N}$). Montrer que $Z + p$ est un multiple de 3.

c. On pose $Z + p = 3q$; ($q \in \mathbb{N}$).

Montrer que (X, Y, Z) solution de (E'') si et seulement si :

$$\begin{cases} Y = 2p + 1 \\ Z = 3q - p \\ X = p + 2q + 2 \end{cases} \quad \text{avec } (p, q) \in \mathbb{Z} \times \mathbb{Z}$$

d. Retrouver alors les solutions de (E) .

Exercice 42

On désigne par A l'ensemble des entiers naturels inférieurs ou égaux à 2010.

1.a. On admet que 2011 est un nombre premier.

Justifier que l'équation $(E) : 67x + 2011y = 1$ admet des solutions dans $\mathbb{Z}$.

b. Vérifier que le couple $(-30; 1)$ est une solution particulière de (E) .

c. Montrer que les solutions de (E) sont les couples $(2011k - 30; -67k + 1)$, $k \in \mathbb{Z}$.

d. Déduire la valeur du naturel $x \leq 2010$ vérifiant $67x \equiv 1 \pmod{2011}$. (x est l'inverse de 67 modulo 2011).

2.a. Soit a un entier, montrer que : $a^2 \equiv 1 \pmod{2011} \Leftrightarrow a \equiv 1 \pmod{2011}$ ou $a \equiv -1 \pmod{2011}$.

b. En déduire que 1 et 2010 sont les seuls entiers de A qui sont égaux à leurs inverses.

3. Montrer alors que $(2010)! \equiv 2010 \pmod{2011}$.

Exercice 43

1. Démontrer que, pour tout entier naturel $n : 2^{3n} - 1$ est un multiple de 7 (on pourra utiliser un raisonnement par récurrence). En déduire que $2^{3n+1} - 2$ est un multiple de 7 et que $2^{3n+2} - 4$ est un multiple de 7.

2. Déterminer les restes de la division par 7 des puissances de 2.

3. Le nombre p étant un entier naturel, on considère le nombre entier : $A_p = 2^p + 2^{2p} + 2^{3p}$.

a) Si $p = 3n$, quel est le reste de la division de A_p par 7?

b) Démontrer que si $p = 3n + 1$ alors A_p est divisible par 7.

c) Étudier le cas où $p = 3n + 2$.

4. On considère les entiers a et b écrits dans le système binaire : $a = \overline{1001001000}$, $b = \overline{1000100010000}$. Vérifier que ces deux nombres sont des nombres de la forme A_p . Sont-ils divisibles par 7?

Exercice 44

1. On cherche deux entiers relatifs x et y solutions de l'équation :

$$(1) \quad ax + by = 60 \quad (a \text{ et } b \text{ entiers naturels donnés tels que } ab \neq 0).$$

On notera d le plus grand commun diviseur de a et b .

a. On suppose que l'équation (1) a au moins une solution (x_0, y_0) .

Montrer que d divise 60.

b. On suppose que d divise 60. Prouver qu'il existe alors au moins une solution (x_0, y_0) à l'équation (1).

2. On considère l'équation : (2) $24x + 36y = 60$. (x et y entiers relatifs).

a. Donner le PGCD de 24 et 36 en justifiant brièvement. Simplifier alors l'équation (2).

b. Trouver une solution évidente pour l'équation (2) et résoudre cette équation. On appellera S l'ensemble des couples $(x; y)$ solutions.

c. Énumérer tous les couples $(x; y)$ solutions de (2) et tels que : $-10 \leq x \leq 10$.

Donner parmi eux, ceux pour lesquels x et y sont multiples de 5.

d. Dans le plan rapporté à un repère orthonormal (unité graph : 1 cm), représenter l'ensemble E des points M de coordonnées $(x; y)$ telles que :

$$\begin{cases} x = 1 + 3t \\ y = 1 - 2t \end{cases}, t \in \mathbb{R}$$

e. Montrer que les points ayant pour coordonnées les solutions $(x; y)$ de l'équation (2) appartiennent à l'ensemble E . Comment peut-on caractériser S ?

Exercice 45

- 1.a. Quel est le reste de la division euclidienne de 6^{10} par 11 ? Justifier.
- b. Quel est le reste de la division euclidienne de 6^4 par 5 ? Justifier.
- c. En déduire que $6^{40} \equiv 1 [11]$ et que $6^{40} \equiv 1 [5]$.
- d. Démontrer que $6^{40} - 1$ est divisible par 55.
2. Dans cette question x et y désignent des entiers relatifs.
- a. Montrer que l'équation $(E): 65x - 40y = 1$ n'a pas de solution.
- b. Montrer que l'équation $(E'): 17x - 40y = 1$ admet au moins une solution.
- c. Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E') .
- d. Résoudre l'équation (E') . En déduire qu'il existe un unique naturel x_0 inférieur à 40 tel que $17x_0 \equiv 1 [40]$.
3. Pour tout entier naturel a , démontrer que si $a^{17} \equiv b [55]$ et si $a^{40} \equiv 1 [55]$, alors $b^{33} \equiv a [55]$.

Exercice 46

Dans cet exercice a et b désignent des entiers strictement positifs.

1. a. Démontrer que s'il existe deux entiers u et v tels que $au + bv = 1$ alors a et b sont premiers entre eux.
- b. En déduire que si $(a^2 + ab - b^2)^2 = 1$ alors a et b sont premiers entre eux.
2. On se propose de déterminer tous les couples d'entiers strictement positifs $(a; b)$ tels que $(a^2 + ab - b^2)^2 = 1$.
1. Un tel couple sera appelé solution.
- a. Déterminer a lorsque $a = b$.
- b. Vérifier que $(1; 1)$, $(2; 3)$ et $(5; 8)$ sont trois solutions particulières.
- c. Montrer que si $(a; b)$ est solution et si $a < b$, alors $a^2 - b^2 < 0$.
3. a. Montrer que si $(x; y)$ est une solution différente de $(1; 1)$ alors $(y - x; x)$ et $(y; y + x)$ sont aussi des solutions.
- b. Déduire de 2. b. trois nouvelles solutions.
4. On considère la suite de nombres entiers strictement positifs $(a_n)_{n \in \mathbb{N}}$ définie par $a_0 = a_1 = 1$ et pour tout entier n :

$$a_{n+2} = a_{n+1} + a_n.$$

Démontrer que pour tout entier naturel n , (a_n, a_{n+1}) est solution. En déduire que les nombres a_n et a_{n+1} sont premiers entre eux.

Exercice 47 (le jour de la semaine correspondant à la date de l'attaque de Tidjikja)

Pour déterminer quel jour de la semaine correspond à une date donnée (bien sûr après l'année 1582), on s'attèle à quatre règles :

Règle 1 : Chaque année comporte au moins 365 jours. Certaines années (années bissextiles) en comportent 366.

Règle 2 : Les années bissextiles sont les années dont le millésime est divisible par 4.

Règle 3 : Exception. Les années dont le millésime est divisible par 100 ne sont pas bissextiles.

Règle 4 : Exception à l'exception. Les années dont le millésime est divisible par 400 sont bissextiles.

1. La nuit du 12 mai 1905 vers vingt et une heures, un commando de résistants à la colonisation française dirigé par Sidi Ould Moulaye Zein fait assaut sur la base militaire de Tidjikja. Le bilan de cette attaque fut très lourd du côté de l'armée coloniale : la mort du général Cappolani et de plusieurs militaires. Ce commando était composé, en plus de Sidi Ould Moulaye Zein, de vaillants hommes qui méritent d'être cités ici : Moulaye Abderrahmane surnommé Lellé (fils de Sidi Ould Moulaye Zein), El Arbi Ould Zeidane (son neveu), Ahmed Ould Bah Ould Chkouna, Mohamed Ould Behnass, Ahmed Ould Lemlih, Cheikh Ould El'iyel, Mohamed Saleck Ould Saleck Ould Battah et son frère Mohamed Mahmoud, Moussa Ould Boubeit, Sidi Ould Boubeit, Sidi Ould Weiss, Ahmed Ould Sidi Ould Bah, Sid'Ahmed Ould Bah Ould Cheikh Ould Boubeit, Ould Saleck, Mohamed Ould Ely Ould Saleck, Mohamed Ould Savra, Ahmed Ould El Harthi, Mohamed Ould Levrak, Ahmed Ould Henoune, Mohamed Ould Meilid, Hmoud Ould Ely et Slaka Ould Dahah.

(Source Nouakchott-Info n° 292 du 16 février 2002)

Quel jour de la semaine était ce 12 mai 1905 ?



2. Le mathématicien français Cédric Villani, en photo ci-contre, a reçu la médaille Fields (c'est la plus haute distinction internationale décernée en mathématiques) en 2010.

Il est considéré comme l'un des plus grands mathématiciens du 21^{ème} siècle. Cédric Villani est né le 5 octobre 1973.

Quel jour de la semaine est-il né ?



3. La mathématicienne iranienne Maryam Mirzakhani, en photo ci-contre, a reçu également la médaille Fields en 2014 pour ses travaux en topologie et elle est considérée comme une sommité dans la communauté scientifique.

Maryam Mirzakhani est née le 5 mai 1977 à Téhéran.

Quel jour de la semaine est-elle née ?



4. « Il n'est pas possible d'être mathématicien sans avoir l'âme d'un poète » telle est la citation choc de la mathématicienne russe Sofia Kovalevskaya (elle signe elle-même Sophie Kowalevski). Fille d'un général russe, Sofia Kovalevskaya est la 1^{ère} femme devenue docteur en mathématiques dans une université allemande. Elle était disciple, à la fois, des mathématiciens Hermann Ludwig von Helmholtz, Leo Königsberger et Karl Weierstrass. Elle a travaillé sur les équations aux dérivées partielles et étudié la rotation d'un corps solide autour d'un point fixe (problème si difficile que l'Académie des sciences de Berlin avait proposé, en 1850, un prix pour sa résolution). Pour son travail original et novateur dans ces domaines, Sofia obtient le prix Bordin de l'Académie des sciences de Paris (1888) puis le prix de l'Académie des sciences de Stockholm l'année suivante. Sofia Kovalevskaya est née à Moscou le 15 janvier 1850 et décédée, à l'âge de 41 ans, à Stockholm le 10 février 1891. A quel jour de la semaine correspond la triste disparition de la brillante Sofia ?

Exercice 48

Voici une démonstration du petit théorème de Fermat due à Leibniz (il n'est pas sûr que ce dernier connaissait celle de Fermat).

On considère l'expression $Z_n = (u_0 + u_1 + \dots + u_n)^p - (u_0^p + u_1^p + \dots + u_n^p)$ où $u_0, u_1, \dots, u_n$ sont des entiers quelconques (dont la somme n'est pas divisible par p) et p un nombre premier.

1. Montrer par récurrence sur n que Z_n est divisible par p .
2. Retrouver ainsi une démonstration du théorème de Fermat.
3. Application : Montrer que l'équation $3x^2 + 3x + 7 = y^3$ n'admet pas de solution dans $\mathbb{Z}^2$.

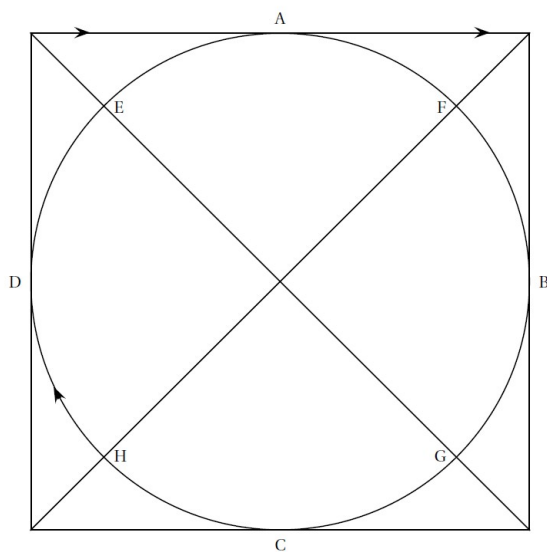
Exercice 49

1. On considère l'équation (E) : $17x - 24y = 9$, où (x, y) est un couple d'entiers relatifs.

a. Vérifier que le couple $(9; 6)$ est solution de l'équation (E).

b. Résoudre l'équation (E).

2. Dans une fête foraine, Jean s'installe dans un manège circulaire représenté par le schéma ci-dessous. Il peut s'installer sur l'un des huit points indiqués sur le cercle.



Le manège comporte un jeu qui consiste à attraper un pompon qui, se déplace sur un câble formant un carré dans lequel est inscrit le cercle. Le manège tourne dans le sens des aiguilles d'une montre, à vitesse constante. Il fait un tour à vitesse constante. Il fait un tour en 24 secondes. Le pompon se déplace dans le même sens à vitesse constante. Il fait un tour en 17 secondes.

Pour gagner, Jean doit attraper le pompon, et il ne peut le faire qu'aux points de contact qui sont notés A, B, C et D sur le dessin. À l'instant $t = 0$, Jean part du point H en même temps que le pompon part du point A .

a. On suppose qu'à un certain instant t Jean attrape le pompon en A . Jean a déjà pu passer un certain nombre de fois en A sans y trouver le pompon.

À l'instant t , on note y le nombre de tours effectués depuis son premier passage en A et x le nombre de tours effectués par le pompon. Montrer que (x, y) est solution de l'équation (E) de la question 1.

b. Jean a payé pour 2 minutes ; aura-t-il le temps d'attraper le pompon ?

c. Montrer, qu'en fait, il n'est possible d'attraper le pompon qu'au point A .

d. Jean part maintenant du point E . Aura-t-il le temps d'attraper le pompon en A avant les deux minutes ?

Exercice 50

1.a. Soit p un entier naturel. Montrer que l'un des trois entiers $p, p + 10$ et $p + 20$, et l'un seulement, est divisible par le nombre 3.

b. Les entiers a, b et c sont dans cet ordre les trois termes consécutifs d'une suite arithmétique de raison 10. Déterminer ces trois termes sachant qu'ils sont premiers.

2. Soit E l'ensemble des triplets d'entiers relatifs (u, v, w) tels que $3u + 13v + 23w = 0$.

a. Montrer que pour un tel triplet $v \equiv w \pmod{3}$.

b. On pose $v = 3k + r$ et $w = 3k' + r$ où k, k' et r sont des entiers relatifs et $0 \leq r \leq 2$.

Montrer que les éléments de E sont de la forme : $(-13k - 23k' - 12r, 3k + r, 3k' + r)$.

c. L'espace est rapporté à un repère orthonormé d'origine O et soit (P) le plan d'équation : $3x + 13y + 23z = 0$. Déterminer l'ensemble des points M à coordonnées (x, y, z) entières relatives appartenant au plan (P) et situés à l'intérieur du cube de centre O , de côté 5 et dont les arêtes sont parallèles aux axes de coordonnées.

Exercice 51

1. Prouver à l'aide du théorème de Fermat que $4^{40} - 1$ est divisible par 41.

2.a. Déterminer le reste de la division euclidienne de 4^n par 17, pour les entiers $n \in \{1, 2, 3, 4\}$.

b. En déduire que le nombre $4^{40} - 1$ est divisible par 17.

3. Prouver que $4^{2^n} - 1$ est divisible par 5 pour tout $n \in \mathbb{N}$.

4. Prouver que $4^n - 1$ est divisible par 3 pour tout $n \in \mathbb{N}$.

5. Déduire des questions précédentes 4 diviseurs premiers de $4^{40} - 1$.

Exercice 52

1. Déterminer tous les entiers naturels a et b tels que $\begin{cases} a \wedge b = 84 \\ a \vee b = 12\,600 \end{cases}$.

2. Soit l'équation (E) : $2x + 3y = 2004$ avec $(x, y) \in \mathbb{N}^2$.

a. Montrer que si (x, y) est solution de (E) alors x est un multiple de 3 et que y est un multiple de 2.

b. Résoudre alors dans $\mathbb{N} \times \mathbb{N}$ l'équation (E).

Exercice 53

On considère dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation diophantienne : (E) $x^2(x^2 + 7) = y(2x + y)$.

Soit (x, y) un élément de $\mathbb{N}^* \times \mathbb{N}^*$ et soit δ le plus grand diviseur commun de x et y . On pose $x = a\delta$ et $y = b\delta$.

1. On suppose que (x, y) est une solution de (E).

a. Vérifier que : $a^2(\delta^2 a^2 + 7) = b(2a + b)$.

b. En déduire qu'il existe un entier naturel k tel que : $2a + b = ka^2$ et $\delta^2 a^2 + 7 = kb$.

c. Montrer que $a = 1$.

d. En déduire que : $(b + 1)^2 = \delta^2 + 8$.

2. Résoudre dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation (E).

Exercice 54

Soit $n \in \mathbb{Z} - \{-2001, 2\}$, on pose : $g(n) = \frac{n+2001}{n-2}$.

1.a. Montrer que : $(n - 2) \wedge (n + 2001) = (n - 2) \wedge 2003$.

b. Vérifier que 2003 est un nombre premier.

c. En déduire les valeurs possibles de $(n - 2) \wedge (n + 2001)$.

d. Déterminer l'ensemble des entiers relatifs n tels que $(n - 2) \wedge (n + 2001) = 2003$.

2. Déterminer les valeurs de n pour lesquelles $g(n) \in \mathbb{Z}$.

3. Soit $p \in \mathbb{N}$ et $q \in \mathbb{N}$ tels que $p \neq q$ et $p \wedge q = 1$.

a. Montrer que $p^2 \wedge (p^2 - q^2) = 1$.

b. Montrer que : $g(n) = \left(\frac{p}{q}\right)^2 \Leftrightarrow n = 2 + \frac{2003}{p^2 - q^2}$.

c. Déterminer p, q et n pour que : $g(n) = \left(\frac{p}{q}\right)^2$ et $p \wedge q = 1$.

Exercice 55

Dans tout l'exercice x et y désignent des entiers naturels non nuls vérifiant $x < y$. Soit S l'ensemble des couples d'entiers (x, y) tels que $x \wedge y = y - x$.

1.a. Calculer $363 \wedge 484$.

b. Le couple $(363, 484)$ appartient-il à S ?

2. Soit $n \in \mathbb{N}^*$; le couple $(n, n+1)$ appartient-il à S ? Justifier votre réponse.

3.a. Montrer que $(x, y) \in S$ si et seulement si il existe $k \in \mathbb{N}^*$ tel que $x = k(y - x)$ et $y = (k + 1)(y - x)$.

b. En déduire que pour tout couple $(x, y) \in S$ on a : $x \vee y = k(k + 1)(y - x)$.

4.a. Déterminer l'ensemble des diviseurs de 228.

b. En déduire l'ensemble des couples (x, y) de S tels que $x \vee y = 228$.

Exercice 56

1. Montrer que : $\forall n \in \mathbb{N}, n + 3$ divise $3n^3 - 11n + 48$.

2. Montrer que pour tout entier n tel que $n \geq 2$, on a : $3n^3 - 11n + 48 \in \mathbb{N}^*$.

3. Montrer que pour tout $(a, b, c) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^*$ tel que $bc \neq a$, on a : $a \wedge b = (bc - a) \wedge b$.

4. Montrer que : $\forall n \in \mathbb{N}^* - \{1\}, (3n^3 - 11n) \wedge (n + 3) = 48 \wedge (n + 3)$.

5. Déterminer l'ensemble des entiers naturels n tels que : $\frac{3n^3 - 11n}{n + 3} \in \mathbb{N}$.

Exercice 57

Soit n un entier naturel premier. On considère dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation : (E) $x^3 - y^3 = n$.

1.a. Montrer que si (x_0, y_0) est une solution de (E) alors :
$$\begin{cases} x_0 - y_0 = 1 \\ x_0^2 + x_0 y_0 + y_0^2 = n \\ 3x_0 y_0 = n - 1 \end{cases}$$

b. Montrer que si $n \neq 3k + 1$ pour tout $k \in \mathbb{N}$ alors l'équation (E) n'admet aucune solution.

c. Montrer que si l'équation (E) admet une solution alors elle est unique.

2. Montrer que si le système $\begin{cases} x - y = 1 \\ 3xy = n - 1 \end{cases}$ admet une solution alors il existe $k \in \mathbb{N}$ tel que : $4n - 1 = 3(2k + 1)^2$.

Exercice 58

Soit a un entier naturel strictement supérieur à 1 et p un entier naturel premier.

1.a. Montrer que pour tous entiers x et y , on a : $\begin{cases} p \wedge x = 1 \\ p \wedge y = 1 \end{cases} \Rightarrow p \wedge (xy) = 1$

b. En déduire que si $p > a$ alors $p \wedge (a!) = 1$.

c. Quels sont les entiers premiers qui divisent $(a!)$?

2. On suppose dans cette question que $p \leq a$ et on cherche à déterminer le plus grand entier α tel que p^α divise $(a!)$ (α est appelé valuation p -adique de $(a!)$).

a. Montrer que les facteurs de $(a!)$ divisibles par p sont les entiers : $p, 2p, 3p, \dots, qp$ où q est le quotient de la division euclidienne de a par p .

b. Vérifier que le produit de tous ces facteurs est $\lambda = (q!)p^q$ et que λ divise $(a!)$.

c. Vérifier que :

→ Si $p > q$ alors $\alpha = q$;

→ Si $p \leq q$ et si q_1 est le quotient de q par p alors p^{q+q_1} divise $(a!)$.

3. On prend $a = 423$ et $p = 7$.

En appliquant les résultats de la question 2., déterminer la valuation 7-adique de $(423!)$ c'est-à-dire le plus grand entier α tel que 7^α divise $(423!)$.

Exercice 59[Ⓢ]

Le but de cet exercice est de déterminer le nombre de "0" que comporte $n!$ à la fin de son écriture décimale. Par exemple $5! = 120$ et donc on a un seul "0" à la fin de son écriture décimale.

1. Montrer que si la décomposition d'un entier a en facteurs premiers est :

$a = 2^{\alpha_1} \times 5^{\alpha_2} \times 7^{\alpha_3} \times \dots$ alors a fini exactement par α_1 ou α_2 "0" dans la base décimale.

2. Soit n un entier naturel non nul.

On pose q_0 le quotient de la division euclidienne de n par 5.

a. Montrer que $n! = 5^{q_0} \cdot (q_0!) \cdot k$; avec $k \in \mathbb{N}$ tel que $k \wedge 5 = 1$.

b. Soit q_1 le quotient de la division euclidienne de q_0 par 5.

Montrer que $n! = 5^{q_0+q_1} \cdot (q_1!) \cdot k_1$; avec $k_1 \in \mathbb{N}$ et $k_1 \wedge 5 = 1$.

c. Expliquer pourquoi le nombre de "0" de $n!$ en base 10 est égal à : $q_0 + q_1 + (\text{nombre de "0" dans } q_1!)$.

3. On définit ainsi une suite réelle q_k définie sur $\mathbb{N}$ par :

$q_0 =$ Le quotient de la division euclidienne de n par 5.

$q_{k+1} =$ Le quotient de la division euclidienne de q_k par 5.

- a. Montrer qu'il existe $n_0 \in \mathbb{N}$ tel que pour tout $k \geq n_0$, on a : $q_k = 0$.
 b. En déduire que le nombre de "0" en base 10 de $n!$ est égal à : $q_0 + q_1 + \dots + q_{n_0}$
4. Application:
 Dans 1960!, il y a combien de fois "0" à la fin de son écriture décimale ?
 Dans 2016!, il y a combien de fois "0" à la fin de son écriture décimale ?

Exercice 60

L'espace est muni d'un repère orthonormé $(0; \vec{i}, \vec{j}, \vec{k})$. Le point F a pour coordonnées $(0, 0, \frac{1}{4})$ et $\mathcal{P}$ le plan d'équation $z = -\frac{1}{4}$. M est un point de l'espace de coordonnées (x, y, z) . H est le projeté orthogonal du point M sur $\mathcal{P}$.

On note $\mathcal{E}$ l'ensemble des points M de l'espace tels que : $MF = MH$.

- Démontrer que $\mathcal{E}$ a pour équation : $x^2 + y^2 = z$.
- a. Quelle est l'intersection de l'ensemble $\mathcal{E}$ et du plan d'équation $z = 2$?
 b. Quelle est l'intersection de l'ensemble $\mathcal{E}$ avec le plan $(0; \vec{j}, \vec{k})$?
- Dans cette question, x et y sont des entiers naturels.
 - Démontrer que 7 divise $x^2 + y^2$ si et seulement si 7 divise x et 7 divise y .
 - Existe-t-il des points qui appartiennent à l'intersection de l'ensemble $\mathcal{E}$ et du plan d'équation $z = 98$ dont toutes les coordonnées sont des entiers naturels ? Si oui, les déterminer.

Exercice 61

- Trouver six entiers strictement positifs et inférieurs à 10 tels qu'aucun d'entre eux n'en divise un autre.
 - Trouver huit entiers strictement positifs et inférieurs à 14 tels qu'aucun d'entre eux n'en divise un autre.
 Il semble que dans tout ensemble de $n + 1$ nombres strictement inférieurs à $2n$, il y en ait toujours un qui en divise un autre. C'est ce que nous allons démontrer.
- Justifier que tout entier strictement positif s'écrit d'une manière unique de la forme d'une puissance de 2 multipliée par un nombre impair.
- Soit $q_1, q_2, \dots, q_{n+1}$ les $n + 1$ nombres considérés. D'après la question 2., on peut donc écrire, pour tout i compris entre 1 et $n + 1$: $q_i = 2^{a_i} \times b_i$ où b_i est un nombre impair et a_i un entier positif ou nul.
 - Combien y a-t-il de nombres impairs inférieurs à $2n$?
 - En déduire que deux des nombres b_i sont égaux entre eux.
- Conclure.

Exercice 62

On pose $a = 7^{2009} + 7^{2010} + 7^{2011}$.

- Soit n un entier naturel. Discuter suivant les valeurs de n , le reste de 7^n modulo 100.
- En déduire qu'il existe un entier naturel k tel que : $a = 100k - 1$.
- a. En utilisant le binôme de Newton, montrer que $a^{100} \equiv 1 \pmod{100^2}$.
 b. Quelles sont les quatre derniers chiffres de a^{100} .

Exercice 63

On pose : $A = 2011^{2011}$.

- Quel est le reste de la division euclidienne de A par 4 ?
- a. Soit n un entier naturel non nul.
 Discuter suivant les valeurs de n le reste de la division euclidienne de 2^n par 7.
 b. Déduire que $A + 5$ est divisible par 7.
 c. Montrer que $A + 5 \equiv 0 \pmod{28}$.
- On pose $B = 2011^n + 2011^{2n} + 2011^{3n}$.
 Déterminer les entiers naturels n pour lesquels B est divisible par 7.

Exercice 64

Soit n un entier naturel.

- Démontrer que le chiffre des unités de n est donné par le reste de la division euclidienne de n par 10
- a. Montrer que $3n \equiv 1 \pmod{10}$ si et seulement si $n \equiv 0 \pmod{4}$
 b. Quel est le chiffre des unités de $N_1 = 3^{1029}$.
 c. Quel est le chiffre des unités de $N_2 = 373^{2531} \times 2353^{190}$
- a. Déterminer, suivant les valeurs de n , le reste modulo 10 de 7^n .
 b. En déduire le chiffre des unités du nombre : 43578707^{4327}
- Soit $n \geq 2$
 a. Démontrer par récurrence que le reste de la division euclidienne de 6^n par 10 est 6.

- b. Quel est le chiffre des unités de 9^n ?
 c. En déduire le chiffre des unités de $N_3 = 426^{1259} \times 859^{12235}$.
 5. Quel est le chiffre des unités de $6^n \times 9^n$?

Exercice 65

- Soit p un entier naturel supérieur ou égal à 2 et k un entier naturel tel que $1 \leq k \leq p-1$.
 a. Démontrer que $k \times C_p^k = p \times C_{p-1}^{k-1}$.
 b. En déduire que si p est un nombre premier, alors p divise C_p^k pour tout entier k vérifiant : $1 \leq k \leq p-1$.
 c. Vérifier ce résultat pour $p = 7$. Que se passe-t-il pour $p = 8$?
- a. On suppose que p est premier. Démontrer par récurrence (sur a) que pour tout entier naturel a , on a la congruence : $a^p \equiv a \pmod{p}$. La propriété est-elle vraie pour un entier relatif quelconque ?
- On suppose toujours que p est premier. Déduire de la question précédente que si a est un entier relatif non multiple de p (et donc premier avec p), on a $a^{p-1} \equiv 1 \pmod{p}$.
- Donner alors les restes des divisions euclidiennes de 2^{340} par 11, par 31, par 341
- Nous venons de démontrer le petit théorème de Fermat, qui peut être énoncé de deux façons différentes.
 Première version : Soit p un entier naturel premier ; alors, pour tout entier relatif a , $a^p \equiv a \pmod{p}$.
 Deuxième version : Soit p un entier naturel premier ; alors, pour tout entier relatif a non multiple de p ,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Les propositions suivantes sont-elles vraies ou fausses ?

- Si a n'est pas multiple de p et si $a^{p-1} \equiv 1 \pmod{p}$, alors p est premier.
- Si p est supérieur ou égal à 2 et s'il existe un entier a premier avec p tel que $a^{p-1} - 1$ n'est pas divisible par p , alors p est composé.

Exercice 66 (Le critère d'Eisenstein)

- Démontrer que, si les entiers p et q sont premiers entre eux, alors pour tout entier naturel n , les entiers p et q^n sont aussi premiers entre eux.
- Soit $n \in \mathbb{N}$ et soient $a_0, a_1, \dots, a_{n-1}, a_n$ des entiers relatifs tels que $a_n \neq 0$. On considère l'équation algébrique de degré n : $(E) \ a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$.
 a. On suppose que (E) admet une solution rationnelle, pouvant donc s'écrire sous la forme d'une fraction irréductible p/q . En appliquant le théorème de Gauss, démontrer que p divise a_0 et que q divise a_n .
 b. Énoncer un critère permettant de connaître les fractions qui peuvent être solutions d'une équation polynomiale, à coefficients entiers. Ce critère est le critère d'**Eisenstein** (mathématicien allemand 1823-1852).
 3. En utilisant le critère d'Eisenstein, résoudre l'équation : $4x^3 - 7x^2 - 12x + 21 = 0$.
- On note $\alpha = \sin\left(\frac{\pi}{18}\right)$.
 a. Exprimer, pour tout réel x , $\sin(3x)$ en fonction de $\sin(x)$.
 b. En déduire que α est solution de l'équation : $(E) \ 4x^3 - 3x + \frac{1}{2} = 0$.
 c. En utilisant le critère d'Eisenstein, démontrer que α est irrationnel.

Exercice 67

L'espace est rapporté au repère orthonormal $(O; \vec{i}, \vec{j}, \vec{k})$.

On nomme (S) la surface d'équation $x^2 + y^2 - z^2 = 1$.

- Montrer que la surface (S) est symétrique par rapport au plan (xOy) .
- On nomme A et B les points de coordonnées respectives $(3; 1; -3)$ et $(-1; 1; 1)$.
 a. Déterminer une représentation paramétrique de la droite (D) passant par les points A et B .
 b. Démontrer que la droite (D) est incluse dans la surface (S) .
- Déterminer la nature de la section de la surface (S) par un plan parallèle au plan (xOy) .
 4. a. On considère la courbe (C) , intersection de la surface (S) et du plan d'équation $z = 68$. Préciser les éléments caractéristiques de cette courbe.
 b. M étant un point de (C) , on désigne par a son abscisse et par b son ordonnée. On se propose de montrer qu'il existe un seul point M de (C) tel que a et b soient des entiers naturels vérifiant $a < b$ et $\text{PPCM}(a; b) = 440$, c'est-à-dire tel que (a, b) soit solution du système $(1) : \begin{cases} a < b \\ a^2 + b^2 = 4\,625 \\ \text{PPCM}(a; b) = 440 \end{cases}$

Montrer que si (a, b) est solution de (1) alors $\text{PGCD}(a; b)$ est égal à 1 ou 5. Conclure.

Exercice 68

Soit a et b deux entiers non nuls et n un entier naturel impair.

- a. Démontrer que $a + b$ divise $a^n + b^n$.
 b. En déduire que 15 divise $2^{45} + 5^{45} + 10^{45} + 13^{45}$.
- Prouver, sans effectuer de division, que 14 divise 1064.

Exercice 69

On considère deux entiers naturels non nuls a et b tels que : $\begin{cases} a^2 + b^2 = 625 \\ a \wedge b = 1 \end{cases}$.

1. Montrer que l'un des nombres a et b est pair et l'autre impair.

2. On suppose que a est pair.

a. Montrer que $(25 - a) \wedge (25 + a) = 1$.

b. Montrer qu'il existe deux entiers naturels impairs m et n tels que : $\begin{cases} 25 + a = m^2 \\ 25 - a = n^2 \\ m \wedge n = 1 \end{cases}$

3. Déterminer a et b .

4. Dédurre de ce qui précède les solutions dans $\mathbb{N}^* \times \mathbb{N}^*$ de l'équation : $x^2 + y^2 = 625$.

Exercice 70

I.1. Trouver tous les couples d'entiers naturels $(a; b)$ tels que : $\begin{cases} a + b = 210 \\ a \wedge b = 15 \end{cases}$

2.a. Calculer en utilisant l'algorithme d'Euclide $2115 \wedge 75$.

b. Déterminer un entier naturel n tel que :

$\begin{cases} \text{Le reste de la division euclidienne de } 2126 \text{ par } n \text{ est } 11 \\ \text{Le reste de la division euclidienne de } 83 \text{ par } n \text{ est } 8 \end{cases}$

II. On donne l'équation (E): $5x - 2y = 1$ où x et y sont deux entiers naturels.

1. Vérifier que le couple $(1, 2)$ est une solution particulière de (E).

2. Résoudre dans $\mathbb{N} \times \mathbb{N}$ l'équation (E).

Soit n un entier naturel, on pose $A = 2n + 3$ et $B = 5n + 2$.

a. Montrer que si un entier naturel non nul d , divise A et divise B alors il divise l'entier 11.

b. Déterminer alors l'ensemble des entiers naturels n tels que : $A \wedge B = 11$.

Exercice 71

On pose $P_n(x) = (x + 1)(x^2 + 1)(x^4 + 1) \cdots (x^{2^n} + 1)$.

1. Simplifier $(x - 1)P_n(x)$.

2. En déduire la forme développée de $P_n(x)$.

3. En déduire que si $F_n = 2^{2^n} + 1$ alors $F_n = F_0 F_1 \cdots F_{n-1} + 2$; où F_n est le $n^{\text{ième}}$ nombre de Fermat.

4. En déduire que si, contrairement à ce qu'espérait Fermat, les nombres de Fermat ne sont pas tous premiers, ils sont au moins premiers entre eux deux à deux.

5. En déduire une autre démonstration du fait qu'il y a un nombre infini de nombres premiers.

Exercice 72

Les entiers entre 2 et n ont en moyenne environ $\ln n$ diviseurs, à un près.

1. Vérifier cette propriété pour $n = 10$.

2. Pour deux entiers naturels i et j , on pose $\delta(i, j) = 1$ si i divise j , et 0 sinon.

Pour un entier naturel n , que représente le nombre : $d(n) = \sum_{i=1}^n \delta(i, n)$?

3. Montrer que $\sum_{j=1}^n \delta(i, j) = \text{partie entière de } \frac{n}{i} = E\left(\frac{n}{i}\right)$.

4. En déduire que la quantité $\overline{d}(n) = \frac{1}{n} \sum_{j=1}^n d(j)$ est comprise entre les deux réels $h_n - 1$ et h_n où h_n est la quantité définie par : $h_n = \sum_{i=1}^n \frac{1}{i}$

5. En utilisant l'encadrement admis $\ln n \leq h_n \leq \ln n + 1$, démontrer la propriété annoncée.

Exercice 73

L'expression d'un entier naturel n , au moyen d'une certaine base de numération b est 1254.

On sait de plus que l'expression de l'entier $2n$ dans la même base est 2541.

1. Déterminer les valeurs de b et n exprimées en base 10.

2. Donner les expressions en base b des entiers $3n$ et $4n$.

Exercice 74

1. Trouver trois entiers naturels a, b, c différents de 1, et premiers entre eux deux à deux tels que $abc = 495$.

2. x, y, z étant des chiffres de la base 10. On considère le nombre $A = \overline{x13y8z}$ en base 10. Déterminer tous les triplets (x, y, z) pour que A soit un multiple de 495.

Exercice 75

1. Le nombre 643 est écrit en base 7. Écrire ce nombre en base 2.

2. Soit a un entier naturel tel que $a > 1$. On considère les nombres $N = 2(a - 1)$ et $N' = (a - 1)^2$. Écrire N et N' dans le système de numération de base a . Vérifier que N et N' s'écrivent avec les mêmes chiffres, mais dans l'ordre inverse.

Exercice 76

1. Trouver tous les entiers naturels dont le cube divise 18360.
2. En déduire dans N , la résolution de l'équation d'inconnue b : $b^3[b^2 + (b + 1)^2] = 18360$.
3. Existe-il un nombre b tel que le nombre qui s'écrit 36723 dans le système décimal s'écrive $\overline{442003}_b$?

Exercice 77

On considère un entier naturel n non nul.

1. Pour $1 \leq n \leq 6$, calculer les restes de la division euclidienne de 3^n par 7.
2. Démontrer que, pour tout entier n , $3^{n+6} - 3^n$ est divisible par 7.
3. En déduire que 3^{n+6} et 3^n ont le même reste dans la division euclidienne par 7.
4. À l'aide des résultats précédents, calculer le reste de la division euclidienne de 3^{2016} par 7.
5. Déterminer, pour tout entier naturel n , le reste de la division euclidienne de 3^n par 7.
6. Pour $n \geq 2$, on pose $u_n = 1 + 3 + 3^2 + \dots + 3^{n-1} = \sum_{k=0}^{n-1} 3^k$.
Montrer que, pour tout naturel $n \geq 2$, u_n est divisible par 7 si et seulement si $3^n - 1$ est divisible par 7.
7. En déduire les valeurs de n pour lesquelles u_n est divisible par 7.

Exercice 78

1. Soit N un entier naturel et S la somme des chiffres de N .
Montrer que N est divisible par 9 si et seulement si S est divisible par 9.
2. On considère le nombre $A = 2009^{2009}$. On désigne par B la somme des chiffres de A , C la somme des chiffres de B et D la somme des chiffres de C .
a. Montrer que $A \equiv D \pmod{9}$.
b. Montrer que A a au plus 8036 chiffres. En déduire que $B \leq 72324$.
c. Montrer que $C \leq 45$.
d. Montrer que $D \leq 12$.
e. En déduire la valeur de D , puis celle de C .

Exercice 79 (Nombres de Mersenne)

On considère les nombres de Mersenne $M_n = 2^n - 1$, pour n entier naturel non nul.

1. a. En utilisant plusieurs valeurs de n , émettre une conjecture sur n pour que le nombre M_n soit un multiple du nombre 3.
b. Démontrer la conjecture à l'aide des congruences.
2. a. Émettre une conjecture sur n pour que M_n soit un nombre premier.
b. Le nombre M_{11} est-il premier ?
c. On suppose que $n = pq$ avec p et q supérieurs ou égaux à 2. Trouver une factorisation de M_n .
d. En déduire que si M_n est premier, alors n est premier. La réciproque est-elle vraie ?
4. On considère les nombres $F_d(x; y) = x^2 + dy^2$ avec d, x et y des entiers naturels.
a. En utilisant les congruences de M_n et $F_1(x; y)$ modulo 4, préciser s'il existe des nombres de Mersenne qui sont la somme de deux carrés d'entiers naturels.
b. Déterminer un entier naturel n et des entiers naturels x et y tels que $M_n = F_2(x; y)$.

Exercice 80 (Nombres de Mersenne, nombres premiers dans une progression arithmétique)

Soit p un nombre premier et x un entier naturel non nul.

Il s'agit de montrer que tout nombre premier divisant $(x + 1)^p - x^p$ est de la forme $np + 1$ et d'examiner quelques applications.

1. Soit q un nombre premier divisant $(x + 1)^p - x^p$.
a. Montrer que $q \geq 3$ et que q est premier avec x .
En déduire que : $x^{p(q-1)} \equiv 1 \pmod{q}$.
b. On pose $a = (x + 1)x^{q-2}$.
Montrer que $a^p \equiv 1 \pmod{q}$ mais que $a \not\equiv 1 \pmod{q}$.
En déduire que l'ordre de a modulo q est égal à p , puisqu'il existe n ($n \geq 1$) tel que $q = np + 1$.
2. Application 1 : On pose $x = N!$ (N entier naturel non nul). Montrer que tout nombre premier divisant $(x + 1)^p - x^p$ est plus grand que N . En déduire qu'il existe une infinité de nombres premiers de la forme $np + 1$.
3. Application 2 : On pose $x = 1$. Montrer que tout nombre premier divisant le nombre $M_p = 2^p - 1$ (avec p premier différent de 2) est de la forme $2kp + 1$ ($k \geq 1$).
On veut savoir « à la main » si M_{11} est composé. Que doit être votre premier essai ?

Exercice 81 (Nombres de Cullen)

1. Soit p un nombre premier impair.

Pour k entier ($k \geq 1$), on pose $n = (p-1)(kp+1)$.

a. Prouver que $n \equiv -1 \pmod{p}$ puis que $2^n \equiv 1 \pmod{p}$.

b. En déduire que p divise $n \cdot 2^n + 1$.

2. Les nombres de la forme $n \cdot 2^n + 1$ sont appelés nombres de Cullen. Montrer que pour tout entier premier impair p , il existe une infinité de nombres de Cullen divisibles par p .

Exercice 82

Soit n un entier naturel supérieur ou égal à 2.

1. Montrer que si a et b sont deux entiers naturels tels que $a > b$, alors $n^a - 1 > n^b - 1$.

2. Montrer que $n^8 - 1 = n^3(n^5 - 1) + n^3 - 1$ est la division euclidienne de $n^8 - 1$ par $n^5 - 1$.

3. Réaliser les calculs de l'algorithme d'Euclide permettant de déterminer : $\text{PGCD}(n^8 - 1; n^5 - 1)$.

4. Comparer avec le PGCD de 8 et 5.

5. Soit a et b deux naturels tels que $a > b > 0$, et $a = bq + r$ la division de a par b et $d = \text{PGCD}(a; b)$.

a. Déterminer l'entier N tel que la division euclidienne de $n^a - 1$ par $n^b - 1$ s'écrive : $n^a - 1 = N(n^b - 1) + n^r - 1$.

b. Déterminer le PGCD de $n^a - 1$ et $n^b - 1$ en fonction de n et de d .

Exercice 83

On admet que 1979 est premier.

1. Résoudre dans $\mathbb{Z}$ l'équation : $2x \equiv 1 \pmod{1979}$.

2. On considère l'équation (E) : $x^2 - x + 494 \equiv 0 \pmod{1979}$.

a. Soit x une solution de l'équation (E) dans $\mathbb{Z}$.

Déterminer le reste de la division euclidienne de $(x - 990)^2$ par 1979.

b. En déduire les solutions de l'équation (E) dans $\mathbb{Z}$.

Exercice 84

1. On considère l'ensemble $A_7 = \{1; 2; 3; 4; 5; 6\}$.

a. Pour tout élément a de A_7 , déterminer l'unique élément y de l'ensemble A_7 tel que $ay \equiv 1 \pmod{7}$.

b. Pour x entier relatif, déterminer a de A_7 tel que l'équation $3x \equiv 5 \pmod{7}$ équivaut à $x \equiv a \pmod{7}$.

c. Si a est un élément de A_7 , montrer que les seuls relatifs x solutions de $ax \equiv 0 \pmod{7}$ sont les multiples de 7.

2. Dans toute cette question, p est un nombre premier supérieur ou égal à 3. On considère l'ensemble $A_p = \{1; 2; \dots; p-1\}$ des entiers naturels non nuls et strictement inférieurs à p . Soit a un élément de A_p .

a. Vérifier que a^{p-2} est solution de l'équation $ax \equiv 1 \pmod{p}$.

b. On note r le reste de la division euclidienne de a^{p-2} par p .

Démontrer que r est l'unique solution x dans A_p tel que $ax \equiv 1 \pmod{p}$.

c. Soient x et y deux entiers relatifs. Démontrer que $xy \equiv 0 \pmod{p}$ ssi x est un multiple de p ou y est un multiple de p .

3. a. Résoudre dans A_{31} les équations : $2x \equiv 1 \pmod{31}$ et $3x \equiv 1 \pmod{31}$.

b. A l'aide des résultats précédents, résoudre dans $\mathbb{Z}$ l'équation suivante : $6x^2 - 5x + 1 \equiv 0 \pmod{31}$.

Exercice 85

Pour tout $n \in \mathbb{N}^*$, on pose $S_n = 1 + 31 + 31^2 + \dots + 31^{n-1}$.

1. Vérifier que $S_{2013} - 31 \times S_{2012} = 1$ puis en déduire que 31 et S_{2013} sont premiers entre eux.

2. Montrer que pour tout $n \geq 1$, $30 \times S_n = 31^n - 1$.

3.a. Vérifier que $31^{2013} \equiv 1 \pmod{S_{2013}}$.

b. Résoudre dans $\mathbb{Z}$ la congruence : $31x \equiv 1 \pmod{S_{2013}}$.

4. On admet que 2011 est premier.

a. Démontrer que si n est premier et $n \geq 7$ alors n divise $S_n - 1$.

b. Déterminer le reste modulo 2011 du nombre S_{2013} .

Exercice 86

1. Étudier suivant les valeurs de l'entier naturel n le reste de la division euclidienne de 5^n par 7.

2. Pour tout entier naturel n , on pose $S_n = 1 + 5 + 5^2 + \dots + 5^n$.

a. Montrer que $4S_n = 5^{n+1} - 1$.

b. Soit a un entier, montrer que : $4S_n \equiv a \pmod{7} \Leftrightarrow S_n \equiv 2a \pmod{7}$.

c. En déduire le reste de la division euclidienne de S_{2010} par 7.

3. Soit n un entier naturel donné.

On considère dans $\mathbb{Z} \times \mathbb{Z}$ les équations : (E_0) : $5^n x - S_n y = 0$ et (E) : $5^n x - S_n y = 7$.

a. Montrer que pour tout entier naturel n , S_n et 5^n sont premiers entre eux.

b. Résoudre l'équation (E_0) .

- c. Montrer que les solutions de (E) sont les $(x; y)$ tels que : $x = 35 + k \times S_n$ et $y = 28 + k \times 5^n$ avec $k \in \mathbb{Z}$
4. Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ le système diophantien : $\begin{cases} 25x - 31y = 7 \\ \text{PGCD}(x; y) = 7 \end{cases}$

Exercice 87

1. Écrire les nombres $1^3, 2^3, 3^3$ comme des différences de deux carrés.
2. Le nombre a est un entier naturel non nul.
 - a. Montrer qu'il existe deux entiers naturels m et p tels que $m + p = a^2$ et $m - p = a$.
 - b. En déduire a^3 en fonction de m et p .
3. Montrer que le cube de tout entier naturel peut s'écrire comme différence de deux carrés.
4. Écrire alors 11^3 comme différence de deux carrés.
5. Démontrer que tout entier naturel impair peut s'écrire comme différence de deux carrés.

Exercice 88

On désigne par p un nombre entier premier supérieur ou égal à 7. Le but de l'exercice est de démontrer que l'entier naturel $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.

1. Montrer que p est congru à -1 ou à 1 modulo 3. En déduire que n est divisible par 3.
2. En remarquant que p est impair, prouver qu'il existe un entier naturel k tel que : $p^2 - 1 = 4k(k + 1)$, puis que n est divisible par 16.
3. En considérant tous les restes possibles de la division de p par 5, démontrer que 5 divise n .
4. a. Soient a, b et c trois entiers naturels. Démontrer que si a divise c et b divise c , avec a et b premiers entre eux, alors ab divise c .
- b. Déduire de ce qui précède que 240 divise n .
5. Existe-t-il quinze nombres premiers $p_1, p_2, \dots, p_{15}$ supérieurs ou égaux à 7 tels que l'entier naturel $A = p_1^4 + p_2^4 + \dots + p_{15}^4$ soit un nombre premier ?

Exercice 89 (Encore l'infinitude des nombres premiers : démonstration de Métrod (en 1917))

Le but de cet exercice est de proposer une autre démonstration de l'existence d'une infinité de nombres premiers. On suppose qu'il n'existe que r ($r \in \mathbb{N}^*$) nombres premiers $p_1, p_2, \dots, p_r$, avec l'ordre $p_1 < p_2 < \dots < p_r$. Soit $N = p_1 \times p_2 \times \dots \times p_r$. On pose $Q_i = \frac{N}{p_i}$ pour tout i appartenant à $\{1; 2; \dots; r\}$, et $S = \sum_{i=1}^r Q_i$.

1. Soit q un entier naturel non nul. Démontrer que si q divise S , alors $q \neq p_i$ pour tout i de $\{1; 2; \dots; r\}$.
2. Conclure.

Exercice 90

On considère les nombres dont l'écriture décimale n'utilise que le chiffre 1.

Pour tout entier naturel $p \geq 2$, on pose $A_p = 11 \dots 1$ (le chiffre 1 apparaît p fois).

- a. On suppose que p est pair. Montrer que A_p est divisible par A_2 .
 - b. On suppose que k est un diviseur de p . Montrer que A_p est divisible par A_k .
2. Soient p et q deux entiers naturels premiers entre eux. On se propose de déterminer $A_p \wedge A_q$. On considère l'équation (E): $px - qy = 1$.
- a. Justifier l'existence des solutions de l'équation (E).
 - b. Vérifier que pour tout $(x; y)$ de naturels solutions de l'équation (E) on a : $(10^{px} - 1) - 10(10^{qy} - 1) = 9$.
 - c. Montrer qu'il existe deux entiers X et Y tels que $A_p X - A_q Y = 1$.
 - d. Déduire des questions précédentes $A_p \wedge A_q$.

Exercice 91® (Une démonstration du petit théorème de Fermat)

1. Soit p un entier naturel supérieur ou égal à 1.

Montrer que $\forall k \in \{1; 2; \dots; p-1\}$, l'entier p divise C_p^k . (Utiliser : $C_p^k = \frac{p!}{k!(p-k)!}$ et le théorème de Gauss.)

- 2.a. Déduire de la question précédente que pour p premier et pour a et b entiers, on a :

$$(a + b)^p = \sum_{k=0}^{k=p} C_p^k a^k b^{p-k} \equiv a^p + b^p \pmod{p}$$

- b. Montrer par récurrence sur k , que : $\forall k \in \mathbb{N}^*$, $\left[\sum_{i=1}^{i=k} a_i \right]^p \equiv \sum_{i=1}^{i=k} a_i^p \pmod{p}$ où les $a_i \in \mathbb{N}$.

En déduire que pour tout entier a , on a : $a^p \equiv a \pmod{p}$.

3. Démontrer que si p est premier et si a n'est pas divisible par p , alors : $a^{p-1} \equiv 1 \pmod{p}$

4. Applications

- a. * Soit p un entier premier tel que $p-1$ divise 2016. Montrer que p divise $n^{2017} - n$.

****** Soit un entier $n \geq 2$, montrer que $n^{2017} - n$ admet au moins 18 diviseurs premiers distincts.
b. Soit n un entier tel que $2n + 1$ est un nombre premier.
Montrer qu'il existe $k \in \mathbb{N}$ tel que $n^n = 2nk + k + 1$ ou $n^n = 2nk + k - 1$.

Exercice 92

- Montrer que pour tout entier naturel a et pour tout entier naturel impair m , on a : $a + 1$ divise $a^m + 1$.
- Soit q un entier naturel premier et $a \in \mathbb{N}$.
a. Montrer que : $(a + 1)^q \equiv a^q + 1 \pmod{q}$.
b. En déduire que : $a^q \equiv a \pmod{q}$.
- Pour tout entier naturel n tel que $n > 1$, on pose : $a_n = (n!)^2 + 1$.
a. Montrer que a_n est impair.
b. Montrer que a_n admet un diviseur premier p tel que $p > n$.
c. On suppose que p s'écrit sous la forme (1) : $p = 4k + 3$ avec $k \in \mathbb{N}$. Montrer que le nombre $1 + (n!)^{2(2k+1)}$ est divisible par a_n et que p divise $n! + (n!)^p$. (On pourra remarquer que $p - 1 = 2(2k + 1)$).
d. En déduire que le nombre p ne peut s'écrire sous la forme (1) ci-dessus.
- Déduire de ce qui précède qu'il y a une infinité de nombres premiers de la forme $4k + 1$ avec $k \in \mathbb{N}$.

Exercice 93 (Entiers naturels sommes de deux entiers)

Dans cet exercice, on se propose d'étudier quelques propriétés des entiers naturels n qui s'écrivent sous la forme $n = a^2 + b^2$ avec a et b entiers naturels. On appellera S l'ensemble des entiers naturels qui peuvent s'écrire ainsi.

- On considère les entiers naturels inférieurs ou égaux à 10. Dresser la liste de ceux qui appartiennent à l'ensemble S .
- Démontrer que tout carré parfait, et que tout entier qui suit un carré parfait, appartiennent à l'ensemble S .
- a. On considère des entiers naturels a, b, c et d . Développer $(ac + bd)^2 + (ad - bc)^2$.
b. En déduire que si $n \in S$ et $p \in S$ alors $n \times p \in S$. (On dit que S est stable pour la multiplication)
c. L'ensemble S est-il stable pour l'addition ?
- Recopier et compléter le tableau suivant pour obtenir la parité de $a^2 + b^2$ à partir de celle des naturels a et b :

a	b	a^2	b^2	$a^2 + b^2$
pair	pair			
impair	impair			
pair	impair			

- On considère un entier N pair appartenant à S . Le but de la question est de démontrer que l'entier $\frac{N}{2}$ appartient également à S . On écrit $N = a^2 + b^2$ avec a et b entiers naturels.
a. A l'aide de la question 4, montrer que a et b ont la même parité. En déduire que $\frac{a+b}{2}$ et $\frac{a-b}{2}$ sont des entiers.
b. Calculer $\left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$.
c. Conclure.
- On considère un entier N impair appartenant à S . Le but de la question est de démontrer que N est de la forme $4k + 1$ avec k entier. On écrit $N = a^2 + b^2$ avec a et b entiers naturels.
a. A l'aide de la question 4, montrer que a et b n'ont pas la même parité. Pour la suite, on supposera par exemple que a est pair et b impair. Il existe donc des entiers u et v tels que $a = 2u$ et $b = 2v + 1$.
b. Calculer $a^2 + b^2$ en fonction de u et v et conclure.
c. Tout entier de la forme $4k + 1$ appartient-il à S ?
d. Le nombre 8 055 appartient-il à S ?

Exercice 94 (Sur la répartition des nombres premiers)

Le but de cet exercice est de démontrer que pour tout entier naturel k non nul, on a $2k - 1 \leq p_k \leq 2^{2^k}$ où p_k désigne le k -ième nombre premier.

- Vérifier que cette double inégalité est vraie pour $k = 1$ et $k = 2$.
- Démontrer par récurrence que : $\forall k \in \mathbb{N}^*, 2k - 1 \leq p_k$
- Soit k un entier naturel non nul et q un nombre premier divisant le nombre $p_1 p_2 \dots p_k + 1$.
a. Démontrer que : $\forall i \in \{1; 2; \dots, k\}, q \neq p_i$
b. En déduire que $p_{k+1} \leq p_1 p_2 \dots p_k + 1$.
- Démontrer par récurrence que : $\forall k \in \mathbb{N}^*, p_k \leq 2^{2^k}$

Exercice 95

1. Soit B une boîte en forme de pave droit de hauteur L , a base carrée de côté l , où l et L sont des entiers naturels non nuls tels que $l < L$. On veut remplir la boîte B avec des cubes tous identiques dont l'arête a est un entier naturel non nul (les cubes devant remplir complètement la boîte B sans laisser d'espace vide).

- a. Dans cette question, $l = 882$ et $L = 945$. Quelle est la plus grande valeur possible pour a ? Quelles sont les valeurs possibles pour a ?
- b. Dans cette question, le volume de la boîte B est $v = 77\,760$. On sait que, pour remplir la boîte B , la plus grande valeur possible de a est 12. Montrer qu'il y a exactement deux boîtes B possibles, dont on donnera les dimensions.
2. On veut remplir une caisse cubique C , dont l'arête c est un entier naturel non nul, avec des boîtes B toutes identiques telles que décrites dans la question 1. (Les boîtes B , empilées verticalement, doivent remplir complètement la caisse C sans laisser d'espace vide).
- a. Dans cette question, $l = 882$ et $L = 945$.
Quelle est la plus petite valeur possible pour c ? Quelles sont les valeurs possibles pour c ?
- b. Dans cette question, le volume de la boîte B est $v = 15\,435$. On sait que la plus petite arête possible pour la caisse C est 105. Quelles sont les dimensions l et L de la boîte B .

Exercice 96[®] (Théorème de Wilson)

Le théorème de Wilson : « p premier $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$ »

Nous allons démontrer dans cet exercice le sens " $\Leftarrow$ " i.e l'implication : $(p-1)! \equiv -1 \pmod{p} \Rightarrow p$ premier

On admet la deuxième implication. Soit p un entier naturel supérieur ou égal à 2.

Supposons que $(p-1)! \equiv -1 \pmod{p}$.

1. Justifier qu'il existe un entier a tel que $(p-1)! \equiv -1 + ap$.

2. Soit k un entier de $\{1; 2; \dots, p-1\}$.

a. En remarquant que l'on peut écrire : $(p-1)! = k \left(\prod_{\substack{1 \leq j \leq p-1 \\ j \neq k}} j \right)$.

montrer que p et k sont premiers entre eux.

b. En déduire que p est premier.

3. Application :

On cherche à déterminer le reste, noté r , dans la division euclidienne de $26!$ par 29.

a. Justifier que 29 divise $28! + 1$.

b. Montrer que $2r \equiv -1 \pmod{29}$.

c. En déduire la valeur de r .

Théorème 97 (théorème de Wilson par les polynômes)

1. Soit p un nombre premier. On considère les polynômes suivants :

$P(X) = (X - (p-1))(X - (p-2)) \cdots (X - 2)(X - 1)$ et $Q(X) = X^{p-1} - 1$.

Montrer que $1, 2, \dots, p-1$ sont racines de Q et en déduire que $P(X) = Q(X)$.

2. En déduire que $(p-1)! \equiv -1 \pmod{p}$.

3. Réciproquement, soit $n \geq 2$ un entier tel que : $(n-1)! \equiv -1 \pmod{n}$. Montrer que n est premier.

4. Déterminer le reste de la division euclidienne de :

a) $26!$ par 29 ;

b) $26!$ par 58.

Exercice 98 (Encore le théorème de Wilson)

1. Soit p un nombre premier ($p \geq 5$) et $A = \{2, \dots, p-2\}$.

Montrer que, pour tout $x \in A$, l'entier $x^2 - 1$ n'est pas divisible par p .

2.a. Soit $x \in A$; prouver qu'il existe un entier u tel que : $xu \equiv 1 \pmod{p}$.

b. En déduire l'existence d'un entier r de A , unique, distinct de x , tel que : $xr \equiv 1 \pmod{p}$.

c. Établir alors que $2 \times \dots \times (p-2) \equiv 1 \pmod{p}$, puis que : $(p-1)! \equiv -1 \pmod{p}$.

3. Ce résultat demeure-t-il vrai lorsque $p = 2$? $p = 3$?

4. Réciproquement, soit p un entier ($p \geq 2$) tel que : $(p-1)! \equiv -1 \pmod{p}$.

En utilisant l'égalité de Bézout, montrer que p est premier.

5. En déduire le théorème de Wilson :

« Un entier p est premier si, et seulement si, $(p-1)! + 1 \equiv 0 \pmod{p}$ » (On n'oubliera pas le cas $p = 2$ et $p = 3$).

Exercice 99

On considère la suite (un) d'entiers naturels définie par : $u_0 = 1$ et, pour tout naturel n , $u_{n+1} = 10u_n + 21$.

1. Calculer u_1 , u_2 et u_3 .

2.a. Démontrer par récurrence que, pour tout entier naturel n : $3u_n = 10^{n+1} - 7$.

b. En déduire, pour tout entier naturel n , l'écriture décimale de u_n .

3. Montrer que u_2 est un nombre premier.

On se propose maintenant d'étudier la divisibilité des termes de la suite (u_n) par certains nombres premiers.

4. Démontrer que, pour tout entier naturel n , u_n n'est divisible ni par 2, ni par 3, ni par 5.

5.a. Démontrer que, pour tout entier naturel n , $3u_n \equiv 4 - (-1)^n \pmod{11}$.

b. En déduire que, pour tout entier naturel n , u_n n'est pas divisible par 11.

6.a. Démontrer que $10^8 \equiv -1 \pmod{17}$ puis que $10^{16} \equiv 1 \pmod{17}$.

b. En déduire que, pour tout entier naturel k , u_{16k+8} est divisible par 17.

Exercice 100

Un écran d'ordinateur est constitué d'un quadrillage, réseau à base carrée ; les carrés appelés "pixels" s'allument individuellement ; ici il y a 640×480 pixels. Les pixels ont pour coordonnées $(x ; y)$ en repère orthonormal où $0 \leq x \leq 640$ et $0 \leq y \leq 480$.

1. On veut tracer sur l'écran le segment d'origine $M(0 ; 319)$ et d'extrémité le point $P(341 ; 0)$.

Déterminer une équation (E) de la droite (MP) de la forme $ax + by = c$ où a, b et c sont des entiers naturels.

2. Calculer PGCD(319 ; 341). Simplifier le plus possible les coefficients de (E).

3. Résoudre l'équation $319x + 341y = 108\,779$, où $(x ; y)$ est un couple d'entiers relatifs.

4. Combien de points à coordonnées entières, M et P mis à part, s'allumeront-ils sur le segment $[MP]$? Montrer que ces points découpent $[MP]$ en des segments de longueur égales.

5. Étude du cas général.

Soient a, b et c trois entiers strictement positifs, avec $\text{PGCD}(a ; b) = 1$.

Montrer que l'équation $ax + by = c$ admet des solutions entières ; donner l'expression générale de ces solutions. En déduire que sur la droite $ax + by = c$, tout segment de longueur supérieure à $\sqrt{a^2 + b^2}$ contient au moins un point à coordonnées entières.

Exercice 101 (La probabilité au secours de l'arithmétique)

On considère un entier n supérieur ou égal à 2 et l'ensemble $S_n = \{1, 2, \dots, n\}$. On considère également la décomposition en produit de facteurs premiers de l'entier n , sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m} \text{ où l'on a } p_1 < p_2 < \dots < p_m$$

Le but de cet exercice est d'établir un résultat qui permet de déterminer le nombre d'entiers de S_n qui sont premiers avec n . On appellera $\varphi(n)$ ce nombre.

1. Dans cette question, on prend $n = 12$.

On a donc $S_{12} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. On prend au hasard, de manière équiprobable, un des entiers de cet ensemble, on appelle X la variable aléatoire égale à la valeur choisie. On a donc par exemple $p(X = 5) = \frac{1}{12}$.

a. Écrire la décomposition en produit de facteurs premiers de 12.

b. On nomme A l'événement « l'entier prélevé est un multiple de 2 » et B l'événement « l'entier prélevé est un multiple de 3 ». Calculer $p(A)$ et $p(B)$.

c. Quelle est la valeur de $\varphi(12)$? On note E l'événement « l'entier prélevé est premier avec 12 ». Calculer $p(E)$.

2. On considère un entier naturel et on suppose que sa décomposition en facteurs premiers est $n = p^\alpha \times q^\beta$ où α, β sont des entiers naturels non nuls.

Comme dans la question 1, on prend au hasard un entiers de manière équiprobable dans l'ensemble

$S_n = \{1, 2, \dots, n\}$. On appelle X la variable aléatoire égale au nombre prélevé.

On nomme C l'événement « l'entier prélevé est un multiple de p », D l'événement « l'entier prélevé est un multiple de q » et F l'événement « l'entier prélevé est premier avec n ».

a. Combien y a-t-il de multiples de p appartenant à S_n ? En déduire que $p(C) = \frac{1}{p}$.

b. Calculer $p(D)$.

c. Démontrer l'équivalence suivante : p et q étant des nombres entiers distincts : $\begin{cases} p/a \\ q/a \\ p \wedge q = 1 \end{cases} \Leftrightarrow p \times q / a$

d. Quel est l'événement $C \cap D$? Combien a-t-il d'éléments ? calculer $p(C \cap D)$.

e. En déduire que C et D sont des événements indépendants.

f. Justifier que $F = \overline{C} \cap \overline{D}$.

d. Déduire des questions précédentes que : $\varphi(n) = n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right)$.

Remarque : Ce résultat se généralise à tout nombre entiers supérieur ou égal à 2 ayant une décomposition en facteurs premiers de la forme $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}$.

On admettra le résultat : $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right)$.

La fonction ainsi définie est appelée indicatrice d'Euler.

Exercice 102

Le plan complexe est rapporté à un repère orthonormal direct.

Soit S la transformation du plan qui, à tout point M d'affixe z , associe le point M' d'affixe z' telle que :

$$z' = 5iz + 6i + 4.$$

Partie A : On note x et x' , y et y' les parties réelles et imaginaires respectives de z et z' . Démontrer que

$$\begin{cases} x' = -5y + 4 \\ y' = 5x + 6 \end{cases}$$

Partie B : Dans cette partie, on se place dans le cas où les coordonnées x et y du point M sont des entiers relatifs tels que $-3 \leq x \leq 5$ et $-3 \leq y \leq 5$. On note (E) l'ensemble de ces points M .

On rappelle que les coordonnées (x', y') du point M' , image du point M par la transformation S , sont :

$$x' = -5y + 4 \text{ et } y' = 5x + 6.$$

1.a. Déterminer l'ensemble des couples (a, b) d'entiers relatifs tels que : $4a + 3b = 5$.

b. En déduire l'ensemble des points M de (E) de coordonnées (x, y) tels que : $-3x' + 4y' = 37$.

2. Soient M un point de l'ensemble (E) et M' son image par la transformation S .

a. Démontrer que $x' + y'$ est un multiple de 5.

b. Démontrer que $x' - y'$ et $x' + y'$ sont congrus modulo 2.

En déduire que si $x'^2 - y'^2$ est un multiple de 2 alors $x' - y'$ et $x' + y'$ le sont également.

c. Déterminer l'ensemble des points M de (E) tels que : $x'^2 - y'^2 = 20$.

Exercice 103

On note E l'ensemble des vingt-sept nombres entiers compris entre 0 et 26.

On note A l'ensemble dont les éléments sont les vingt-six lettres de l'alphabet et un séparateur entre deux mots, noté « * » considéré comme un caractère.

Pour coder les éléments de A , on procède de la façon suivante :

• Premièrement: On associe à chacune des lettres de l'alphabet, rangées par ordre alphabétique, un nombre entier naturel compris entre 0 et 25, rangés par ordre croissant. On a donc $a \rightarrow 0, b \rightarrow 1, \dots, z \rightarrow 25$. On associe au séparateur « * » le nombre 26.

a	b	c	d	e	f	g
0	1	2	3	4	5	6
o	p	q	r	s	t	u
14	15	16	17	18	19	20

h	i	j	k	l	m	n
7	8	9	10	11	12	13
v	w	x	y	z	*	
21	22	23	24	25	26	

On dit que a a pour rang 0, b a pour rang 1, ..., z a pour rang 25 et le séparateur « * » a pour rang 26.

• Deuxièmement: à chaque élément x de E , l'application g associe le reste de la division de $4x + 3$ par 27.

On remarquera que pour tout x de E , $g(x)$ appartient à E .

• Troisièmement : Le caractère initial est alors remplacé par le caractère de rang $g(x)$.

Exemple : $s \rightarrow 18, g(18) = 21$ et $21 \rightarrow v$. Donc la lettre s est remplacée lors du codage par la lettre v .

1. Trouver tous les entiers x de E tels que $g(x) = x$ c'est-à-dire invariants par g .

En déduire les caractères invariants dans ce codage.

2. Démontrer que, pour tout entier naturel x appartenant à E et tout entier naturel y appartenant à E , si on a $y \equiv 4x + 3$ (modulo 27) alors $x \equiv 7y + 6$ (modulo 27). En déduire que deux caractères distincts sont codés par deux caractères distincts.

3. Proposer une méthode de décodage.

4. Décoder le mot « vfv ».

Exercice 104 (Chiffrement avec le code ASCII)

En informatique, le code ASCII (lire : aski) associe à chaque caractère (lettre, chiffre de ponctuation, ...) un entier compris entre 0 et 255 que l'on appelle son code ASCII (American Standard Code for Information Interchange : Code américain normalisé pour l'échange d'information).

La fonction `code` du tableur Excel renvoie le code ASCII du caractère.

Le codage des caractères **Math** est le suivant :

M	a	t	h
77	97	116	104

On décide de crypter le code ASCII par la fonction de cryptage f définie ainsi :

Pour tout entier n tel que $0 \leq n \leq 255$, $f(n)$ est le reste de la division euclidienne de $7n$ par 256.

1. Vérifier que le codage du mot « Math » devient : 27 – 167 – 44 – 216.

2. Soient m et n deux entiers compris entre 1 et 255.

- Montrer que : Si $f(n) = f(m)$ alors $7(n - m) \equiv 0 \pmod{256}$.
- En déduire que deux caractères différents sont codés par deux entiers différents.
- Justifier l'existence d'un couple d'entiers relatifs (u, v) tel que $256u + 7v = 1$.
- Vérifier que $(-5, 183)$ est un tel couple.
- En déduire que $183 \times f(n) \equiv n \pmod{256}$.
- Définir alors une fonction de décryptage g .
- Vérifier que $g(27) = 77$.

Exercice 105

Partie A : Afin de crypter un message, on utilise un chiffrement affine. Chaque lettre de l'alphabet est associée à un nombre entier comme indiqué dans le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Soit x le nombre associé à la lettre à coder. On détermine le reste y de la division euclidienne de $7x + 5$ par 26, puis on en déduit la lettre associée à y (c'est celle qui code la lettre d'origine).

Exemple : M correspond à $x = 12$: $7 \times 12 + 5 = 89$. Or $89 \equiv 11 \pmod{26}$ et 11 correspond à la lettre L , donc la lettre M est codée par la lettre L .

- Coder la lettre L .
- Soit k un entier relatif. Montrer que si $k \equiv 7x \pmod{26}$ alors $15k \equiv x \pmod{26}$.
 - Démontrer que la réciproque de l'implication précédente.
 - En déduire que $y \equiv 7x + 5 \pmod{26}$ équivaut à $x \equiv 15y + 3 \pmod{26}$.
- A l'aide de la question précédente, décoder la lettre E .

Partie B : On considère les suites (a_n) et (b_n) tels que a_0 et b_0 sont des entiers compris entre 0 et 25 inclus et pour tout entier naturel n , $a_{n+1} = 7a_n + 5$ et $b_{n+1} = 15b_n + 3$.

Montrer que pour tout entier naturel n , $a_n = \left(a_0 + \frac{5}{6}\right) \times 7^n - \frac{5}{6}$.

On admet pour la suite du problème que pour tout entier naturel n , $b_n = \left(b_0 + \frac{3}{14}\right) \times 15^n - \frac{3}{14}$.

Partie C : Déchiffrer un message codé avec un chiffrement affine ne pose pas de difficulté (on peut tester les 312 couples de coefficients possibles). Afin d'augmenter cette difficulté de décryptage, on propose d'utiliser une clé qui indiquera pour chaque lettre le nombre de fois où on lui applique le chiffrement affine de la partie A.

Par exemple pour coder le mot $MATH$ avec la clé 2-2-5-6, on applique « 2 » fois le chiffrement affine à la lettre M (cela donne E), « 2 » fois le chiffrement à la lettre A , « 5 » fois le chiffrement à la lettre T et enfin « 6 » fois le chiffrement à la lettre H . Dans cette partie, on utilisera la clé 2-2-5-6. Décoder la lettre Q dans le mot $IYYQ$.

Exercice 106

On se propose dans cet exercice d'étudier le problème suivant : « Les nombres dont l'écriture décimale n'utilise que le seul chiffre 1 peuvent-ils être premiers ? » Pour tout entier naturel $p \geq 2$, on pose $N_p = 11 \dots 1$ où 1 apparaît p fois. On rappelle dès lors que $N_p = 10^{p-1} + 10^{p-2} + \dots + 10^0$.

- Les nombres $N_2 = 11$, $N_3 = 111$ et $N_4 = 1111$ sont-ils premiers ?
- Prouver que $N_p = \frac{10^p - 1}{9}$. Peut-on être certain que $10^p - 1$ est divisible par 9 ?
- On se propose de démontrer que si p n'est pas premier, alors N_p n'est pas premier.

On rappelle que pour tout nombre réel x et tout entier naturel n non nul :

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1).$$

- On suppose que p est pair et on pose $p = 2q$, où q est un entier naturel plus grand que 1. Montrer que N_p est divisible par $N_2 = 11$.
- On suppose que p est un multiple de 3 et on pose $p = 3q$, où q est un entier naturel plus grand que 1. Montrer que N_p est divisible par $N_3 = 111$.
- On suppose que p n'est pas premier et on pose $p = kq$, où k et q sont des entiers naturels plus grands que 1. En déduire que N_p est divisible par N_k .
- Énoncer une condition nécessaire pour que N_p soit premier. Cette condition est-elle suffisante ?

Exercice 107

On considère la suite d'entiers $(a_n)_{n \geq 1}$ définie par $a_n = \overline{111 \dots 11}$ (l'écriture décimale de a_n est composée de n chiffres 1). On se propose de montrer que l'un, au moins, des termes de la suite est divisible par 2 001.

- En écrivant a_n sous la forme d'une somme de puissances de 10, montrer que pour tout naturel n non nul :

$$a_n = \frac{10^n - 1}{9}$$

2. On considère la division euclidienne par 2 001 : expliquer pourquoi parmi les 2 002 premiers termes de la suite, il en existe deux, au moins ayant le même reste.

Soit a_n et a_p deux termes de la suite admettant le même reste ($n < p$).

Quel est le reste de la division euclidienne de $a_n - a_p$ par 2 001 ?

3. Soit k et m deux entiers strictement positifs vérifiant $k < m$.

Démontrer l'égalité $a_m - a_k = a_{m-k} \cdot 10^k$.

4. Calculer le PGCD de 2 001 et de 10.

Montrer que si 2 001 divise $a_m - a_k$, alors 2 001 divise a_{m-k} .

5. Démontrer alors que l'un, au moins, des termes de la suite est divisible par 2 001.

Exercice 108

On rappelle la propriété, connue sous le nom de petit théorème de Fermat :

« soit p un nombre premier et a un entier naturel premier avec p ; alors $a^p - 1$ est divisible par p ».

1. Soit p un nombre premier impair.

a. Montrer qu'il existe un entier naturel k , non nul, tel que $2^k \equiv 1 [p]$.

b. Soit k un naturel non nul tel que $2^k \equiv 1 [p]$ et soit n un naturel. Montrer que si k divise n , alors $2^n \equiv 1 [p]$.

c. Soit b tel que $2^b \equiv 1 [p]$, b étant le plus petit entier non nul vérifiant cette propriété. Montrer, en utilisant la division euclidienne de n par b , que si $2^n \equiv 1 [p]$, alors b divise n .

2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$.

On prend pour p un facteur premier de A .

a. Justifier que : $2^q \equiv 1 [p]$.

b. Montrer que p est impair.

c. Soit b tel que $2^b \equiv 1 [p]$, b étant le plus petit entier non nul vérifiant cette propriété. Montrer en utilisant 1) que b divise q . En déduire que $b = q$.

d. Montrer que q divise $p - 1$, puis montrer que $p \equiv 1 [q]$.

3. Soit $A_1 = 2^{17} - 1$. Voici la liste des nombres premiers de la forme $34m + 1$ et qui sont inférieurs à 400, avec m entier non nul : 103, 137, 239, 307. En déduire que A_1 est premier.

Exercice 109 (La règle de Luhn)

Un numéro de carte bancaire est de la forme : $\overline{a_{15}a_{14} \dots a_2a_1a_0}$ où $a_0, a_1, \dots, a_{15}$ sont des entiers compris entre les entiers 0 et 9. A chaque entier a_i du numéro, on associe le nombre $m(a_i)$ défini de la façon suivante :

$$\begin{cases} m(a_i) = 2a_i & \text{si } 0 \leq 2a_i \leq 9 \\ m(a_i) = \alpha + \beta & \text{si } 2a_i = \overline{\alpha\beta} \end{cases}$$

1. Démontrer que $0 \leq m(a_i) \leq 9$.

2. Tout numéro de carte bancaire doit vérifier la règle de Luhn suivante :

$$a_0 + m(a_1) + a_2 + m(a_3) + \dots + a_{14} + m(a_{15}) \equiv 0 \pmod{12}$$

a. Vérifier que le numéro 4 978 210 033 328 381 respecte cette règle.

b. Démontrer que si un chiffre et un seul est erroné, l'erreur est détectée.

c. Démontrer que la permutation de deux chiffres successifs distincts du numéro est détectée, sauf dans un seul cas. Lequel ?

Exercice 110

1. On considère l'équation (E) : $109x - 226y = 1$ où x et y sont des entiers relatifs.

a. Déterminer le PGCD de 109 et 226. Que peut-on en conclure pour l'équation (E) ?

b. Montrer que l'ensemble des solutions de (E) est l'ensemble des couples de la forme

$$(141 + 226k, 68 + 109k) \text{ où } k \text{ appartient à } \mathbb{Z}.$$

En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109d = 1 + 226e$. (On précisera les valeurs des entiers d et e).

2. Démontrer que 227 est un nombre premier.

3. On note A l'ensemble des 227 entiers naturels a tels que $a \leq 226$. On considère les deux fonctions f et g de A dans A définies de la manière suivante :

à tout entier de A , f associe le reste de la division euclidienne de a^{109} par 227.

à tout entier de A , g associe le reste de la division euclidienne de a^{141} par 227.

a. Vérifier que $g[f(0)] = 0$. On rappelle le résultat suivant appelé petit théorème de Fermat : « Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1$ modulo p . »

b. Montrer que, quel que soit l'entier non nul a de A , $a^{226} \equiv 1$ (modulo 227).

c. En utilisant 1.b., en déduire que, quel que soit l'entier naturel non nul a de A , $g[f(a)] = a$.

Que peut-on dire de $f[g(a)] = a$?

Exercice 111

Partie A : On considère l'équation (E) : $11x - 26y = 1$, où x et y désignent deux nombres entiers relatifs.

1. Vérifier que le couple $(-7; -3)$ est solution de (E).
2. Résoudre alors l'équation (E).
3. En déduire le couple d'entiers relatifs $(u; v)$ solution de (E) tel que : $0 \leq u \leq 25$.

Partie B : On assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On « code » tout nombre entier x compris entre 0 et 25 de la façon suivante :

- on calcule $11x + 8$;
 - on calcule le reste de la division euclidienne de $11x + 8$ par 26, que l'on appelle y .
- x est alors « codé » par y . Ainsi, par exemple, la lettre L est assimilée au nombre 11.
 $11 \times 11 + 8 = 129$ or $129 \equiv 25 \pmod{26}$; 25 est le reste de la division euclidienne de 129 par 26.
 Au nombre 25 correspond la lettre Z. La lettre L est donc codée par la lettre Z.
1. Coder la lettre W.
 2. Le but de cette question est de déterminer la fonction de décodage.
 - a. Montrer que pour tous nombres entiers relatifs x et j , on a : $11x \equiv j \pmod{26}$ équivaut à $x \equiv 19j \pmod{26}$.
 - b. En déduire un procédé de décodage.
 - c. Décoder la lettre W.

Exercice 112

1. On se propose, dans cette question, de déterminer tous les entiers relatifs N tels que : $\begin{cases} N \equiv 5 \pmod{13} \\ N \equiv 1 \pmod{17} \end{cases}$
 - a. Vérifier que 239 est solution du système.
 - b. Soit N un relatif solution de ce système. Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux relatifs vérifiant $17x - 13y = 4$.
 - c. Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.
 - d. En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.
 - e. Démontrer l'équivalence entre $N \equiv 18 \pmod{221}$ et $\begin{cases} N \equiv 5 \pmod{13} \\ N \equiv 1 \pmod{17} \end{cases}$.
2. a. Existe-t-il un entier naturel k tel que $10^k \equiv 1 \pmod{17}$?
 b. Existe-t-il un entier naturel ℓ tel que $10^\ell \equiv 18 \pmod{221}$?

Exercice 113

Le but de l'exercice est de montrer qu'il existe un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009 \pmod{10000}$.

Partie A

1. Déterminer le reste de la division euclidienne de 2009^2 par 16.
2. En déduire que $2009^{8001} \equiv 2009 \pmod{16}$.

Partie B : On considère la suite (u_n) définie par : $u_0 = 2009^2 - 1$ et, pour tout naturel n , $u_{n+1} = (u_n + 1)^5 - 1$.

1. a. Démontrer que u_0 est divisible par 5.
 b. Démontrer, que pour tout entier naturel n : $u_{n+1} = u_n[u_n^4 + 5(u_n^3 + 2u_n^2 + 2u_n + 1)]$.
 c. Démontrer par récurrence que, pour tout entier naturel n , u_n est divisible par 5^{n+1} .
 2. a. Vérifier que l'on a $u_3 = 2009^{250} - 1$ puis en déduire qu'on aussi : $2009^{250} \equiv 1 \pmod{625}$.
 b. Démontrer alors que $2009^{8001} \equiv 2009 \pmod{625}$.

Partie C

1. En utilisant le théorème de Gauss et les résultats établis dans les questions précédentes, montrer que : $2009^{8001} - 2009$ est divisible par 10 000.
2. Conclure, c'est-à-dire déterminer un entier naturel dont l'écriture décimale du cube se termine par 2009.

Exercice 114[Ⓢ] (Quelques aspects arithmétiques de la suite de Fibonacci)

Soit (F_n) la suite de Fibonacci, définie par : $F_0 = 0$, $F_1 = 1$ et $\forall n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.

1. Montrer que $\forall n > 0$, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. En déduire que F_n et F_{n+1} sont premiers entre eux.
2. Montrer que $\forall n > 0$ et $\forall p \in \mathbb{N}$, on a $F_{n+p} = F_p F_{n+1} + F_{p-1} F_n$. (On pourra faire une récurrence sur p)
 En déduire que $\text{PGCD}(F_n, F_p) = \text{PGCD}(F_{n+p}, F_p)$.
3. Soit $a \in \mathbb{N}$, $b \in \mathbb{N}^*$. Si r désigne le reste de la division euclidienne de a par b , montrer que : $\text{PGCD}(F_a, F_b) = \text{PGCD}(F_b, F_r)$
4. Montrer que $\forall (n, p) \in \mathbb{N}^2$, $\text{PGCD}(F_n, F_p) = F_{\text{PGCD}(n, p)}$.

☞ On pourra s'inspirer de l'algorithme d'Euclide.

En déduire la valeur de $\text{PGCD}(F_{2016}, F_{105})$.

5. Étant donné un entier naturel $a \geq 2$ quelconque, on cherche à démontrer qu'il existe un entier n non nul tel que a divise F_n . On note $\bar{F}_k$ le reste dans la division euclidienne de F_k par a .

a. Justifier que $\bar{F}_k$ appartient à l'ensemble $I_a = \{0, 1, \dots, a-1\}$. On peut donc noter les $\bar{F}_k : \bar{F}_0, \bar{F}_1, \dots, \bar{F}_{a-1}$.

b. Montrer que pour tout $k \in \{0, 1, \dots, a-3\}$, on a : $\bar{F}_{k+2} = \bar{F}_{k+1} + \bar{F}_k$.

c. On sait que pour tout entier p , il existe $m \in \{0, 1, \dots, a-1\}$ tel que : $F_p \equiv \bar{F}_m [a]$

Montrer par récurrence que : $\forall k \in \{0, 1, \dots, m\}, F_{p-k} \equiv \bar{F}_{m-k} [a]$.

d. En prenant $k = m$ dans la dernière congruence, conclure.

e. Application : Montrer qu'il existe un terme de la suite de Fibonacci dont l'écriture décimale se termine par 2016 zéros.

Exercice 115^{⊗⊗} (Une démonstration originale de l'infinitude des nombres premiers)

Le but de cet exercice est de démontrer que l'ensemble des nombres premiers est infini.

Pour cela, on va démontrer que si l'ensemble des nombres premiers est fini, alors on ne peut pas décomposer en facteurs premiers tous les entiers naturels de 1 à n pour n « assez » grand.

On note P l'ensemble des nombres premiers et on suppose que l'ensemble P est fini. On peut alors écrire : $P = \{p_1; p_2; \dots, p_k\}$, où k est un entier naturel non nul et $p_1 < p_2 < \dots < p_k$.

Soit n un entier naturel fixé, on suppose que la décomposition en facteurs premiers de n s'écrit :

$$n = p_1^{\alpha_1(n)} \times p_2^{\alpha_2(n)} \times \dots \times p_k^{\alpha_k(n)} \text{ où } \alpha_i(n) \text{ est un entier naturel éventuellement nul.}$$

1. Démontrer que pour tout i de $\llbracket 1; k \rrbracket$: $p_i^{\alpha_i(n)} \leq n$.

2. a. Démontrer que pour tout i de $\llbracket 1; k \rrbracket$: $\alpha_i(n) \leq \frac{\ln(n)}{\ln(p_i)}$.

b. En déduire que pour tout i de $\llbracket 1; k \rrbracket$: $\alpha_i(n) \leq \frac{\ln(n)}{\ln(2)}$.

c. Soit m un entier naturel inférieur ou égal à n et $\alpha_i(m)$ l'exposant de p_i dans la décomposition en facteurs premiers de l'entier m . Donner un majorant de $\alpha_i(m)$.

3. On a supposé que l'ensemble P est fini et contient k nombres premiers distincts deux à deux. Donc décomposer un entier m inférieur ou égal à n , c'est choisir un k -uplet de la forme : $(\alpha_1(m); \alpha_2(m); \dots; \alpha_k(m))$.

a. Démontrer que le nombre de ces k -uplets est majoré par $\left(\frac{\ln(n)}{\ln(2)}\right)^k$.

b. Démontrer qu'alors : $n \leq \left(\frac{\ln(n)}{\ln(2)}\right)^k$.

4. a. Démontrer que la quantité : $\frac{\left(\frac{\ln(n)}{\ln(2)}\right)^k}{n}$ tend vers 0 lorsque n tend vers $+\infty$.

b. En déduire que si n est « assez grand », alors : $n > \frac{\left(\frac{\ln(n)}{\ln(2)}\right)^k}{n}$.

5. Conclure.

Exercice 116[⊗] (Le théorème d'Euler)

Le but de cet exercice est de démontrer un théorème dû à Euler qui généralise le petit théorème de Fermat :

« Pour tout entier $m \geq 2$, pour tout entier a premier avec m , on a : $a^{\varphi(m)} \equiv 1 [m]$. »

$\varphi(n)$ étant le nombre d'entiers naturels strictement inférieurs à n et premiers avec n .

φ ainsi définie sur $\mathbb{N}^*$ (par convention $\varphi(1) = 1$) est appelée fonction indicatrice d'Euler.

On a $\varphi(n) \geq 2$, pour tout $n \geq 3$.

1. Démontrer ce théorème pour $m = 2$.

2. On suppose désormais que $m \geq 3$. Soit $a \in \mathbb{N}^*$ premier avec m .

On note $n_1, n_2, \dots, n_{\varphi(m)}$ les $\varphi(m)$ entiers naturels compris entre 1 et $m-1$ et premiers à m , rangés dans l'ordre croissant. Pour $k \in \{1, 2, \dots, \varphi(m)\}$, on note alors r_k le reste de la division euclidienne de $a \times n_k$ par m .

a. Démontrer que, pour $1 \leq k \leq \varphi(m)$, $r_k \neq 0$.

b. Démontrer que, pour $1 \leq k \leq \varphi(m)$: r_k est premier à m .

c. Démontrer que, pour $1 \leq k' \leq \varphi(m)$ et $k' \neq k$: $r_k \neq r_{k'}$.

d. En déduire que : $r_1 \times r_2 \times \dots \times r_{\varphi(m)} \equiv n_1 \times n_2 \times \dots \times n_{\varphi(m)} [m]$.

Puis que : $a^{\varphi(m)} \times n_1 \times n_2 \times \dots \times n_{\varphi(m)} \equiv n_1 \times n_2 \times \dots \times n_{\varphi(m)} [m]$.

e. Conclure.

Annexe

Annexe

Démonstrations des théorèmes du cours d'Arithmétique

Propriété d'Archimède :

Étant donnés deux entiers $0 < a < b$, il existe un entier n tel que $b < na$.

Preuve :

Comme $0 < a$ et a entier alors $a \geq 1$ et donc $a \cdot b \geq b$. Donc $n = b + 1$ convient car :

$$a(b + 1) = a \cdot b + a > a \cdot b \geq b.$$

I. DIVISIBILITE DANS $\mathbb{Z}$

Propriétés :

Les lettres a et b désignent des entiers relatifs.

- ✓ Pour tout entier n , on a toujours $1 / n, (-1) / n$.
- ✓ Pour tout entier non nul n , on a toujours n / n et $(-n) / n$.
- ✓ Les seuls diviseurs de 1 ou (-1) sont 1 et (-1).
- ✓ Si a / b et b / c alors a / c (propriété de transitivité).
- ✓ Si a / b et $b \neq 0$ alors $|a| \leq |b|$. Ainsi, tout entier non nul admet un nombre fini de diviseurs.
- ✓ Dans $\mathbb{Z}$, on a : si a / b et b / a alors $a = b$ ou $a = -b$.
- ✓ Dans $\mathbb{N}$, on a : si a / b et b / a alors $a = b$.
- ✓ Si a / b et a / c alors $a / [\alpha b + \beta c]$ pour tous entiers relatifs α et β .

Preuves :

Les propriétés 1, 2 et 3 sont évidentes.

4. Si a / b et si b / c alors il existe deux entiers q et r tels que $b = aq$ et $c = br$ donc $c = (aq)r = a(qr)$. D'où a / c .
5. Si a / b et $b \neq 0$ alors il existe un entier q non nul tel que $b = aq$ donc $|b| = |a| \times |q|$ et $|q| \geq 1$ d'où $|b| \geq |a|$.
6. Si a / b et b / a alors $|a| \leq |b|$ et $|b| \leq |a|$ donc $|a| = |b|$, soit $a = \pm b$.
7. Ce cas se déduit du point 6.
8. Si a / b et a / c alors il existe deux entiers q et r tels que $b = aq$ et $c = ar$ donc :

$$\alpha b + \beta c = \alpha(aq) + \beta(ar) = a(\alpha q + \beta r)$$
 donc $a / (\alpha b + \beta c)$.

II. NOMBRES PREMIERS

Théorème 1

1. Tout entier naturel n autre que 1 admet au moins un diviseur premier.
2. Tout entier naturel n , autre que 0 et 1 et non premier, admet au moins un diviseur premier p tel que $p^2 \leq n$.

Preuves :

1. 2 divise 0, donc 0 admet au moins un diviseur premier : l'entier 2.
 Soit n un entier naturel autre que 0 et 1 et D_n l'ensemble des diviseurs naturels de n strictement supérieurs à 1. Comme n est un diviseur de n , donc D_n est une partie non vide de $\mathbb{N}$. On en déduit que D_n possède un plus petit élément p tel que p est un diviseur naturel de n , et $p > 1$.
 On considère un diviseur naturel de p ; soit d tel que $1 \leq d \leq p$.
 Comme d divise p et p divise n , alors d divise n . Or p est le plus petit des diviseurs naturels de n , autre que 1 ; soit donc $d = 1$ ou $d = p$.
 L'entier p ne possède donc que deux diviseurs naturels 1 et p , ce qui signifie que p est premier.
 Ainsi l'entier n , autre que 0 et 1 ; admet au moins un diviseur premier p .
2. On suppose n entier naturel, autre que 0 et 1, et non premier ; alors le plus petit des diviseurs naturels de n , autre que 1, est un entier p tel que $1 < p < n$.
 Comme p divise n , il existe un entier q tel que $n = pq$. L'entier q n'est pas nul, car $n \neq 0$, et n'est pas égal à 1, car $n \neq p$; donc $q > 1$. De plus $p > 1$, donc $pq > q$, c'est-à-dire $n > q$. Ainsi $1 < q < n$ et q divise n .
 On en déduit que q est un diviseur de n , strictement supérieur à 1 : $q \in D_n$. Comme p est le plus petit des éléments de D_n , nécessairement $p \leq q$; donc $p^2 \leq pq$, c'est-à-dire $p^2 \leq n$.

Théorème 2

L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Preuve :

Raisonnons par l'absurde en supposant que l'ensemble des nombres premiers est fini. Notons dans ce cas $p_1, p_2, \dots, p_r$ la liste complète des nombres premiers et posons $N = (p_1 \times p_2 \times \dots \times p_r) + 1$. On a $N \in \mathbb{N}$ et $N \geq 2$, donc l'entier naturel N admet au moins un diviseur premier p_k , avec $k \in \llbracket 1, r \rrbracket$. Alors p_k divise N et p_k divise $p_1 \times p_2 \times \dots \times p_r = N - 1$; d'où p_k divise $N - (N - 1) = 1$. Voilà une belle contradiction.

Lemme 1

Soit $r \in \mathbb{N}^*$, $p_1, p_2, \dots, p_r$ des nombres premiers tels que $p_1 < p_2 < \dots < p_r$ et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls. Alors tout diviseur premier de $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ est l'un des p_i , $i \in \llbracket 1, r \rrbracket$.

Preuve :

Notons $\mathcal{D}$ l'ensemble des entiers naturels de la forme $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ (avec $p_1 < p_2 < \dots < p_r$ et $\alpha_1, \alpha_2, \dots, \alpha_r$ des entiers naturels non nuls) dont au moins un diviseur premier n'est pas l'un des p_i , $i \in \llbracket 1, r \rrbracket$. Montrons que l'ensemble $\mathcal{D}$ est vide.

Raisonnons par l'absurde en supposant $\mathcal{D}$ non vide. Alors $\mathcal{D}$ est une partie non vide de $\mathbb{N}$ et possède donc un plus petit élément $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ dont un certain diviseur premier p n'est aucun des p_i , $i \in \llbracket 1, r \rrbracket$.

Par hypothèse, $p / p_1(p_1^{\alpha_1-1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r})$, et par ailleurs p et p_1 , en tant que nombres premiers distincts, sont premiers entre eux, donc via le théorème de Gauss, on a $p / p_1^{\alpha_1-1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$. Or $p_1^{\alpha_1-1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ n'est pas élément de $\mathcal{D}$ car $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ en est le plus petit. Par conséquent, puisque $p / p_1^{\alpha_1-1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$, p est l'un des p_i , $i \in \llbracket 1, r \rrbracket$, ce qui est contradictoire et nous permet de conclure que $\mathcal{D} = \emptyset$.

Théorème 3 (théorème fondamental de l'arithmétique)

Tout entier naturel $n \geq 2$ s'écrit de manière unique sous la forme de sa décomposition en facteurs premiers $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$ où $p_1 < p_2 < \dots < p_r$ sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ sont des entiers naturels non nuls.

Preuve :

→ **Existence** : Notons $\mathcal{E}$ l'ensemble des nombres premiers supérieurs ou égaux à 2, impossibles à décomposer en un produit de nombres premiers. Montrons que l'ensemble $\mathcal{E}$ est vide.

Raisonnons par l'absurde en supposant que $\mathcal{E}$ est non vide. Alors $\mathcal{E}$ est une partie non vide de $\mathbb{N}$ et possède un plus petit élément $n \geq 2$. Deux cas se présentent alors : soit n est premier, soit n est composé. Or n ne peut pas être premier car il serait aussitôt décomposable en produit de nombres premiers (un produit d'un seul nombre). Donc le nombre n est composé. Il s'écrit alors $n = ab$ où a et b sont deux diviseurs positifs de n autres que n et 1. Remarquant alors que $a < n$ et $b < n$, on peut affirmer que ni a , ni b n'est élément de $\mathcal{E}$, puisque n est le plus petit élément. Par suite, a et b sont des produits de nombres premiers, et il en est de même de leur produit ab . Ceci contredit la définition de n , car $n = ab$.

Conclusion : $\mathcal{E}$ est vide, autrement dit tout entier naturel supérieur ou égal à 2 est produit de nombres premiers.

→ **Unicité** : Notons $\mathcal{F}$ l'ensemble des entiers naturels supérieurs ou égaux à 2 qui possèdent au moins deux décompositions différentes en produit de nombres premiers. Montrons que $\mathcal{F}$ est vide.

Raisonnons par l'absurde en supposant $\mathcal{F}$ non vide. Alors $\mathcal{F}$ est une partie non vide de $\mathbb{N}$ et possède un plus petit élément $n \geq 2$. Soit $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r} = q_1^{\beta_1} \times q_2^{\beta_2} \times \dots \times q_s^{\beta_s}$ deux décompositions distinctes de n en produit de nombres premiers - avec bien sûr $p_1 < p_2 < \dots < p_r$ et $q_1 < q_2 < \dots < q_s$. Alors grâce au lemme 1, on peut affirmer que $q_1 = p_i$, pour un certain $i \in \llbracket 1, r \rrbracket$ et $p_1 = q_j$, pour un certain $j \in \llbracket 1, s \rrbracket$. On a donc :

$$p_1 = q_j \geq q_1 = p_i \geq p_1, \quad \text{et} \quad \text{donc} \quad p_1 = q_1.$$

Du coup :

$$\frac{n}{p_1} = p_1^{\alpha_1-1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r} = q_1^{\beta_1-1} \times q_2^{\beta_2} \times \dots \times q_s^{\beta_s}.$$

Or $\frac{n}{p_1}$ n'est pas un élément de $\mathcal{F}$ puisque n en est le plus petit élément, et donc $\frac{n}{p_1}$ possède une unique décomposition en produit de nombres premiers. On en déduit donc que $r = s$ et que $p_i = q_i$ pour tout $i \in \llbracket 1, r \rrbracket$. Ceci contredit finalement le fait que les décompositions $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r} = q_1^{\beta_1} \times q_2^{\beta_2} \times \dots \times q_s^{\beta_s}$ ont été choisies distinctes.

Conclusion : $\mathcal{F}$ est vide ; autrement dit tout entier naturel supérieur ou égal à 2 est produit de nombres premiers d'une et une seule façon.

III. DIVISION EUCLIDIENNE

Théorème

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

- $a = bq + r$;
- $0 \leq r < b$.

Preuve :

→ **Existence du couple (q, r)** : On démontre d'abord l'existence de (q, r) dans le cas où $a \geq 0$. Introduisons pour cela l'ensemble $E = \{k \in \mathbb{N} / a - bk \geq 0\}$. Cet ensemble E est une partie non vide de $\mathbb{N}$ - non vide car $0 \in E$. Mais par ailleurs E est majoré par a . En effet, soit $k \in E$; alors $a - bk \geq 0$, donc $k \leq bk \leq a$. L'ensemble E possède donc un plus grand élément q . Alors $a - bq \geq 0$. Mais comme $(q + 1) \notin E$, on a : $a - b(q + 1) < 0$. Ces deux dernières inégalités s'écrivent encore : $0 \leq a - bq \leq b - 1$.

Posons donc $r = a - bq$. Alors notre couple (q, r) a été trouvé.

Étendons maintenant le résultat au cas où $a < 0$. Or si $a < 0$ alors $-a > 0$ et on est ramené au cas précédent : il existe un couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $-a = bq + r$ et $0 \leq r \leq b - 1$. Là encore, deux cas peuvent être distingués :

1. Si $r = 0$, posons $q' = -q$ et $r' = 0$. Alors $a = -bq - r = -bq = bq' + r'$ et $0 \leq r' \leq b - 1$.
2. Si $r \geq 1$, posons $q' = -q - 1$ et $r' = b - r$. Alors $a = -bq - r = (-bq - b) + (b - r) = bq' + r'$ et $0 \leq r' \leq b - 1$.

Et nous voilà donc arrivés à CQFD.

→ **Unicité du couple (q, r)** : Soit deux couples (q, r) et $(q', r') \in \mathbb{Z} \times \mathbb{N}$ tels que : $a = bq + r = bq' + r'$, $0 \leq r \leq b - 1$ et $0 \leq r' \leq b - 1$. Alors $|r' - r| \leq b - 1$, mais par ailleurs $b(q - q') = r' - r$.

Supposons $q \neq q'$. Alors $|r' - r| \geq 1$, donc $b|q - q'| \geq b$. On a donc : $b \leq b|q - q'| = |r' - r| \leq b - 1$, donc on a la contradiction : $b \leq b - 1$. Donc $q = q'$. On en déduit aussitôt que :

$$r = a - bq = a - bq' = r'$$

Ce qui achève la démonstration.

IV. CONGRUENCES

On adopte la **définition** suivante :

Soit n un entier naturel supérieur ou égal à 2. Deux entiers a et b sont congrus modulo n lorsque $a - b$ est divisible par n . On note $a \equiv b [n]$.

Théorème 1

Soit n un entier naturel supérieur ou égal à 2.

Deux entiers a et b sont congrus modulo n , si et seulement si, la division euclidienne de a par n a le même reste que la division euclidienne de b par n .

Preuve :

- Si $r = r'$:

$$a - b = nq + r - nq' - r' = n(q - q') \text{ donc } a - b \text{ est divisible par } n \text{ et donc } a \equiv b [n].$$

- Si a et b sont congrus modulo n :

$$a - b = nq + r - nq' - r' = n(q - q') + r - r'. \text{ Donc } r - r' = a - b - n(q - q') \text{ et comme } a \equiv b [n], \text{ alors } a - b \text{ est divisible par } n \text{ et donc } r - r' \text{ est divisible par } n. \text{ Par ailleurs, } 0 \leq r < n \text{ et } 0 \leq r' < n,$$

$$\text{Donc } -n < r' - r < n.$$

Le nombre $r - r'$ est un multiple de n strictement compris entre $-n$ et n , d'où $r - r' = 0$, soit $r = r'$.

Théorème 2 (Réduction modulo n)

Soit n un entier naturel supérieur ou égal à 2.

Si r est le reste de la division euclidienne de l'entier a par n alors $a \equiv r [n]$.

Preuve :

En effectuant la division euclidienne de a par n , on trouve : $a = qn + r$ avec $0 \leq r < n$. Comme $a - r = qn$ est un multiple de n alors $a \equiv r [n]$. Dans ce cas r est le plus entier naturel congru à a modulo n .

Propriétés

Les lettres a, b, c, d désignent des entiers relatifs ; n et p des entiers naturels avec $n \geq 2$.

1. $a \equiv a [n]$
2. $\begin{cases} a \equiv b [n] \\ b \equiv c [n] \end{cases} \Rightarrow a \equiv c [n]$ (transitivité de la congruence)
3. $\begin{cases} a \equiv c [n] \\ b \equiv d [n] \end{cases} \Rightarrow a + b \equiv c + d [n]$ (compatibilité de la congruence avec l'addition)
4. $\begin{cases} a \equiv c [n] \\ b \equiv d [n] \end{cases} \Rightarrow a - b \equiv c - d [n]$ (compatibilité de la congruence avec la soustraction)
5. $\begin{cases} a \equiv c [n] \\ b \equiv d [n] \end{cases} \Rightarrow a \times b \equiv c \times d [n]$ (compatibilité de la congruence avec la multiplication)
6. $a \equiv b [n] \Rightarrow a^p \equiv b^p [n]$

Preuve :

1. $a - a = 0$ est divisible par n .
2. $a \equiv b [n]$ et $b \equiv c [n]$ donc n divise $a - b$ et $b - c$ et par conséquent n divise $(a - b) + (b - c) = a - c$.
3. $a \equiv c [n]$ et $b \equiv d [n]$ donc n divise $a - c$ et $b - d$ et par conséquent n divise $(a - c) + (b - d)$ c'est-à-dire n divise $(a + b) - (c + d)$.
4. $b \equiv d [n]$ signifie que n divise $d - b = (-b) - (-d)$ et donc $-b \equiv -d [n]$. On se ramène au cas 3.
5. On remarque que $cd - ab = c(d - b) + b(c - a)$. Du coup, si $a \equiv c [n]$ et $b \equiv d [n]$ alors n divise $c - a$ et $d - b$ et par suite n divise $c(d - b) + b(c - a)$.
6. Raisonnons par récurrence sur p .
Initialisation : la démonstration est triviale pour $p = 0$ ou $p = 1$

Hérédité : supposons qu'il existe un entier k tel que la propriété soit vraie : $a^k \equiv b^k [n]$

Démontrons que : La propriété est vraie au rang $k + 1$: $a^{k+1} \equiv b^{k+1} [n]$.

$$a^{k+1} = a \times a^k \equiv a \times b^k = b^{k+1} [n]$$

Conclusion :

La propriété est vraie pour $p = 0$ et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel p .

V. PGCD – PPCM

Propriétés :

Pour tous entiers relatifs a, b et k , on a :

1. $\text{PGCD}(a ; 0) = |a|$ (avec $a \neq 0$).
2. Si $b|a$ alors $\text{PGCD}(a ; b) = |b|$.
3. Si r est le reste dans la division euclidienne de a par b alors : $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$.
4. $\text{PGCD}(a ; b) = \text{PGCD}(|a| ; |b|)$.
5. d diviseur commun de a et $b \Leftrightarrow d$ divise $\text{PGCD}(a ; b)$.
6. Si $d = \text{PGCD}(a ; b)$ alors il existe deux entiers relatifs u et v tels que $d = a.u + b.v$. (Identité de Bézout)
7. $\text{PGCD}(ka ; kb) = |k| \times \text{PGCD}(a ; b)$.
8. $\text{PGCD}(a ; b) \times \text{PPCM}(a ; b) = |a| \times |b|$.

Preuves :

1. $|a|$ est le plus grand diviseur de a , et c'est naturellement un diviseur de 0.
2. $|b|$ est le plus grand diviseur de b et c'est également un diviseur de a car b divise a .
3. On note respectivement q et r le quotient et le reste de la division euclidienne de a par b . Si D un diviseur de b et r alors D divise $a = bq + r$ et donc D est un diviseur de a et b . Réciproquement, si D un diviseur de a et b alors D divise $r = a - bq$ et donc D est un diviseur de b et r . On en déduit que l'ensemble des diviseurs communs de a et b est égal à l'ensemble des diviseurs communs de b et r . Et donc en particulier, on a : $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$.
4. Il est évident que l'ensemble des diviseurs communs de a et b n'est que l'ensemble des diviseurs communs de $|a|, |b|$.
5. La preuve se lit en trois étapes. On note $D(x)$ l'ensemble des diviseurs de l'entier x .

Étape 1 :

Étant donnés deux entiers naturels a et b , avec b non nul, on fait la division euclidienne de a par b . On a : $a = b.q_0 + r_0$ avec $0 \leq r_0 < b$ et on démontre que $D(a) \cap D(b) = D(b) \cap D(r_0)$ (voir la propriété V.3).

Étape 2 :

Si $r_0 \neq 0$ on recommence l'étape 1 avec le couple $(b; r_0)$. $b = q_1 \cdot r_0 + r_1$ avec $0 \leq r_1 < r_0$. On a alors $D(a) \cap D(b) = D(b) \cap D(r_0) = D(r_0) \cap D(r_1)$. Et ainsi de suite, on construit une suite d'entiers $r_0, r_1, \dots, r_n$ vérifiant $0 \leq r_n < r_{n-1} < \dots < r_1 < r_0$ et $D(a) \cap D(b) = D(r_{n-1}) \cap D(r_n)$. Ce processus est nécessairement fini car (r_n) est une suite strictement décroissante d'entiers naturels.

Étape 3 :

La dernière étape a lieu lors de l'apparition du premier reste nul.

Si $r_n = 0$ avec $r_{n-1} \neq 0$ on a $D(a) \cap D(b) = D(r_{n-1}) \cap D(0) = D(r_{n-1})$ car $D(0) = \mathbb{N}$.

Le PGCD de a et de b est donc égal au dernier reste non nul obtenu dans les divisions successives.

6. On se limite dans cette démonstration au cas où a et b sont des entiers naturels car si l'un de ces entiers est négatif, on peut faire « ingurgiter » son signe au coefficient u ou v correspondant.

Soit $E = \{n \cdot a + m \cdot b \mid n \in \mathbb{Z} \text{ et } m \in \mathbb{Z}\}$. On a : $E \cap \mathbb{N}^* \neq \emptyset$ car $a \in E$ (prendre $n = 1$ et $m = 0$)

$E \cap \mathbb{N}^*$ étant une partie non vide de $\mathbb{N}$ possède un plus petit élément ; notons-le d.

Comme $d \in E$ il existe deux entiers relatifs u et v tels que $d = a \cdot u + b \cdot v$.

- E contient clairement tous les multiples de d.

- Réciproquement, soit x un élément de $E \cap \mathbb{N}^*$.

Il existe deux entiers q et r tels que : $x = dq + r$ avec $0 \leq r < d$. Alors $r = x - dq$ donc $r \in E$ (différence de deux éléments de E). Si r était non nul, on aurait $r \in E \cap \mathbb{N}^*$; impossible car $r < d$ (plus petit élément de $E \cap \mathbb{N}^*$), donc $r = 0$. Par suite x est un multiple de d.

On a prouvé que $E \cap \mathbb{N}^*$ est l'ensemble des multiples de son plus petit élément d.

Montrons que d est le PGCD de a et de b. Soit $d' = a \wedge b$

- d'/a et d'/b donc $d' / a \cdot u + b \cdot v$ et par suite d' / d .

- d/a et d/b donc d / d' (propriété V.5)

On a d'/d et d/d' et donc enfin $d = d'$.

7. Soit $k \in \mathbb{Z}$. Nous pouvons supposer $k \neq 0$. Notons $\delta = \text{PGCD}(a; b)$ et $\Delta = \text{PGCD}(ka; kb)$.

On a d'une part δ/a et δ/b , donc $k\delta/ka$ et $k\delta/kb$, donc par définition de Δ , $k\delta/\Delta$.

D'autre part, k/ka et k/kb , donc par définition de Δ , k/Δ , de sorte qu'il existe $n \in \mathbb{Z}$ tel que $\Delta = nk$. Il vient ensuite que nk/ka et nk/kb , donc n/a et n/b car $k \neq 0$. Par définition de δ , cela montre que n/δ , puis, en multipliant par k, que $nk/k\delta$ soit $\Delta/k\delta$.

Nous obtenons ainsi la double divisibilité $k\delta/\Delta$ et $\Delta/k\delta$, et donc $|\Delta| = |k\delta|$, ou encore $\Delta = |k|\delta$.

8. Comme $\text{PGCD}(a; b) = \text{PGCD}(|a|; |b|)$, on peut se limiter au cas où a et b sont des entiers naturels tels que l'un au moins d'entre eux n'est pas nul.

On pose $\begin{cases} \delta = a \wedge b \\ \mu = a \vee b \end{cases}$ et a' et b' tels que $\begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$

Les entiers a' et b' sont premiers entre eux sinon il existerait un entier $d \geq 2$ qui diviserait a' et b'. Dans ce cas

l'entier $d\delta$ vérifie : $d\delta > \delta$ et $\begin{cases} d\delta/a \\ d\delta/b \end{cases}$ ce qui est contradictoire à la définition de δ . Donc, on bien $a' \wedge b' = 1$.

Remarquons que $\delta \cdot a' \cdot b'$ est un multiple commun à a et b et donc à μ , donc : $\exists k \in \mathbb{N}$ tel que $\delta \cdot a' \cdot b' = k \cdot \mu$.

Comme μ est un multiple commun à a et b, on a d'autre part : $\begin{cases} \mu = \alpha a \\ \mu = \beta b \end{cases}$.

Ainsi : $\begin{cases} b' = k\alpha \\ a' = k\beta \end{cases}$ Or, comme $a' \wedge b' = 1$ alors $k = 1$. Et donc : $\delta \cdot a' \cdot b' = \mu$.

On conclut en multipliant par δ .

VI. THEOREME BEZOUT – THEOREME DE GAUSS

Théorème 1 (théorème de Bézout)

Soient a et b des entiers relatifs.

$a \wedge b = 1 \Leftrightarrow$ Il existe 2 entiers u et v tels que $au + bv = 1$.

Preuve :

$\Leftarrow$ Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Soit D le PGCD de a et b, alors D divise a et D divise b, donc D divise $au + bv$. Donc D divise 1. Donc $D = 1$.

On en déduit alors que a et b sont premiers entre eux.

$\Rightarrow$ Supposons que a et b sont premiers entre eux.

Considérons l'ensemble E des entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

E n'est pas vide (E contient a ou $-a$, E contient b ou $-b$, ...), donc E a un plus petit élément m .
On peut écrire $m = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.
Écrivons la division euclidienne de a par m : $a = mq + r$ avec $r \in \mathbb{N}$ et $0 \leq r < m$.
Donc $a = (au_1 + bv_1)q + r$, d'où $r = a - (au_1 + bv_1)q = a(1 - u_1q) + b(-v_1q)$.
Donc r est un entier naturel de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ et d'autre part $r < m$.
Comme m est le plus petit élément de E , on en déduit que $r = 0$, c'est-à-dire que a est divisible par m .
De même on démontrerait que b est divisible par m .
Donc m est un diviseur commun à a et b .
Comme a et b sont premiers entre eux, on en déduit que $m = 1$.
On a donc $1 = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Théorème 2

Soit a et b deux entiers naturels.

$$a \wedge b = d \Leftrightarrow \exists a' \text{ et } b' \in \mathbb{N} \text{ tels que } \begin{cases} a = a'd \\ b = b'd \\ a' \wedge b' = 1 \end{cases}$$

Preuve :

$\Rightarrow$ Soient a, b des entiers relatifs non nuls et D un entier naturel non nul.

Supposons que $D = \text{PGCD}(a; b)$ alors D divise a et D divise b ,

donc $a = Da'$ et $b = Db'$ avec a' et b' entiers relatifs non nuls,

donc $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls.

Soit $d \in \mathbb{N}$ un diviseur commun à $\frac{a}{D}$ et $\frac{b}{D}$, alors $\frac{a}{D} = da''$ et $\frac{b}{D} = db''$ avec $a'' \in \mathbb{Z}^*$ et $b'' \in \mathbb{Z}^*$.

donc $a = dDa''$ et $b = dDb''$, donc dD est un diviseur commun à a et b .

Comme D est le PGCD, on en déduit que $d = 1$.

On a démontré que dans $\mathbb{N}$ le seul diviseur commun à $\frac{a}{D}$ et $\frac{b}{D}$ est 1, donc $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux.

$\Leftarrow$ Supposons que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.

Puisque $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers, D divise a et D divise b .

Soit $g = \text{PGCD}(a; b)$.

D divise a et b , donc D divise g et donc $D \leq g$.

D'autre part $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux, donc il existe des entiers relatifs u et v tels que $\frac{a}{D}u + \frac{b}{D}v = 1$.

donc $D = au + bv$.

Mais g étant le PGCD de a et de b , g divise a et b , donc g divise $au + bv$ donc g divise D , donc $g \leq D$.

On a donc finalement $g = D$, c'est-à-dire $D = \text{PGCD}(a; b)$

On a donc démontré que :

$$D = \text{PGCD}(a; b) \Leftrightarrow \frac{a}{D} \text{ et } \frac{b}{D} \text{ sont des entiers relatifs non nuls premiers entre eux}$$

Théorème 3 (théorème de Gauss)

a, b et c sont trois entiers relatifs avec $ab \neq 0$

$$\text{Si } \begin{cases} a \text{ divise } b \times c \\ a \wedge b = 1 \end{cases} \text{ alors } (a \text{ divise } c)$$

Preuve :

a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que : $au + bv = 1$.

Alors $acu + bcv = c$. On sait que a divise bc , donc a divise bcv .

D'autre part a divise acu . Donc a divise $acu + bcv$ c'est-à-dire a divise c .

Théorème 4 (conséquence du théorème de Gauss)

$$\text{Si } \begin{cases} a \text{ et } b \text{ divisent } c \\ a \wedge b = 1 \end{cases} \text{ alors } a \times b \text{ divise } c$$

Preuve :

a et b divisent c donc il existe des entiers a' et b' tels que : $c = a \times a' = b \times b'$.

Alors a divise $b \times b'$ et est premier avec b donc, d'après le théorème de Gauss, a divise b' . Donc il existe un entiers k tel que $b' = k \times a$. Ainsi $c = b \times b' = k \times ab$, donc ab divise c .

Théorème 5 (Lemme d'Euclide)

a et b sont des entiers relatifs et p un nombre premier.

Si $\begin{cases} p \text{ est premier} \\ p \text{ divise } a \times b \end{cases}$ alors $(p \text{ divise } a) \text{ ou } (p \text{ divise } b)$

Preuve :

Supposons que p ne divise pas a , alors $a \neq 0$ et a et p sont premiers entre eux (puisque p est premier) donc p divise ab et p est premier avec a , donc p divise b d'après le théorème de Gauss.

Théorème 6 (Petit théorème de Fermat)

Soit a un entier relatif et p un entier naturel.

Si $\begin{cases} p \text{ est premier} \\ p \text{ ne divise pas } a \end{cases}$ alors $a^{p-1} \equiv 1 \pmod{p}$ (c'est-à-dire $p \mid a^{p-1} - 1$)

Preuve :

Pour chaque entier k compris entre 1 et $p - 1$, notons r_k le reste de la division euclidienne de $k \times a$ par l'entier p . Ainsi, $ka \equiv r_k \pmod{p}$ et $0 \leq r_k \leq p - 1$.

Justifions que $r_k \neq 0$. On raisonne par l'absurde: si $r_k = 0$, p divise $k \times a$; or, p est premier et ne divise pas a , donc p est premier avec a ; alors, selon le théorème de Gauss, p divise k . Mais ceci est impossible, car k est compris entre 1 et $p - 1$. Montrons que tous les r_k sont distincts deux à deux.

Si $ka \equiv r_k \pmod{p}$ et $k'a \equiv r_{k'} \pmod{p}$, alors $(k - k')a \equiv 0 \pmod{p}$; si $k' \neq k$ alors comme p ne divise pas a , le recours au théorème de Gauss nous conduit à une contradiction. Comme k prend les $p - 1$ valeurs distinctes de 1 à $p - 1$ et qu'à chaque k correspond un reste différent r_k alors r_k prend toutes les valeurs possibles de 1 à $p - 1$.

Multipliant les $p - 1$ relations $ka \equiv r_k \pmod{p}$ pour $1 \leq k \leq p - 1$. Alors, on obtient : $(p - 1)! a^{p-1} \equiv (p - 1)! \pmod{p}$.

Donc p divise $(p - 1)! (a^{p-1} - 1)$. Or, p ne figure dans aucune des décompositions des facteurs du produit $(p - 1)!$, donc p ne divise pas $(p - 1)!$, donc p est premier avec $(p - 1)!$; donc, selon le théorème de Gauss, p divise $a^{p-1} - 1$.

VII. SYSTÈME DE NUMERATION A BASE B**Théorème**

Soit b un entier naturel autre que 0 et 1.

Soit un entier naturel non nul N . On peut écrire N de manière unique sous la forme :

$$N = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 \quad (1)$$

avec les a_k des entiers vérifiant : $0 < a_n < b$ et $\forall i \in \llbracket 1, n - 1 \rrbracket, 0 \leq a_i < b$.

Preuve :

→ **Existence** : Notons pour cela $P(N)$ la propriété : « N possède une écriture de la forme (1) comme indiqué dans le libellé du théorème ». La propriété $P(1)$ est vraie, avec $n = 0$ et $a_0 = 1$. Considérons alors un entier $N \geq 2$ et supposons que la propriété $P(k)$ soit vraie pour tout entier k tel que $1 \leq k < N$. Il s'agit de démontrer que $P(N)$ est vraie. Tel est le cas si l'on a $N < b$, en prenant $n = 0$ et $a_0 = N$ dans (1).

Supposons donc $N \geq b$. Il existe des entiers q et a_0 tels que l'on ait : $N = bq + a_0$ avec $0 \leq a_0 < b$. L'inégalité $N \geq b$ entraîne $q \geq 1$. Par suite, $q < qb \leq N$. La propriété $P(q)$ étant vraie, il existe un entier $n \geq 1$ tel que l'on ait : $q = a_n b^{n-1} + \dots + a_2 b + a_1$, où les a_i sont des entiers vérifiant $0 \leq a_i \leq b - 1$ et où $a_n \neq 0$. L'égalité $N = bq + a_0$ entraîne alors que $P(N)$ est vraie.

→ **Unicité** : On remarque pour établir l'unicité de la décomposition que l'entier n intervenant dans la relation (1) vérifie les inégalités : $b^n \leq N < b^{n+1}$.

En effet, la première inégalité est immédiate et le fait que les a_i soient compris entre 1 et $b - 1$ entraîne que l'on a les inégalités : $N \leq (b - 1)(b^n + b^{n-1} + \dots + b + 1) = b^{n+1} - 1 < b^{n+1}$.

Remarque hors démonstration :

$$b^n \leq N < b^{n+1} \Rightarrow n \cdot \log b \leq \log N < (n + 1) \log b$$

$$\Rightarrow n \leq \frac{\log N}{\log b} < n + 1$$

$$\Rightarrow \text{Partie entière de } \frac{\log N}{\log b} = n$$

Donc pour tout entier $N \geq 1$, le nombre de chiffres intervenant dans l'écriture de N en base b est donné par :

$$E\left(\frac{\log N}{\log b}\right) + 1$$

où $E(x)$ désigne la partie entière de x et $\log$ désigne une fonction logarithme quelconque (en pratique, on prend la fonction logarithme de base b car dans ce cas $\log b = 1$, ce qui facilite les calculs).

Tout revient donc à démontrer que si l'on a :

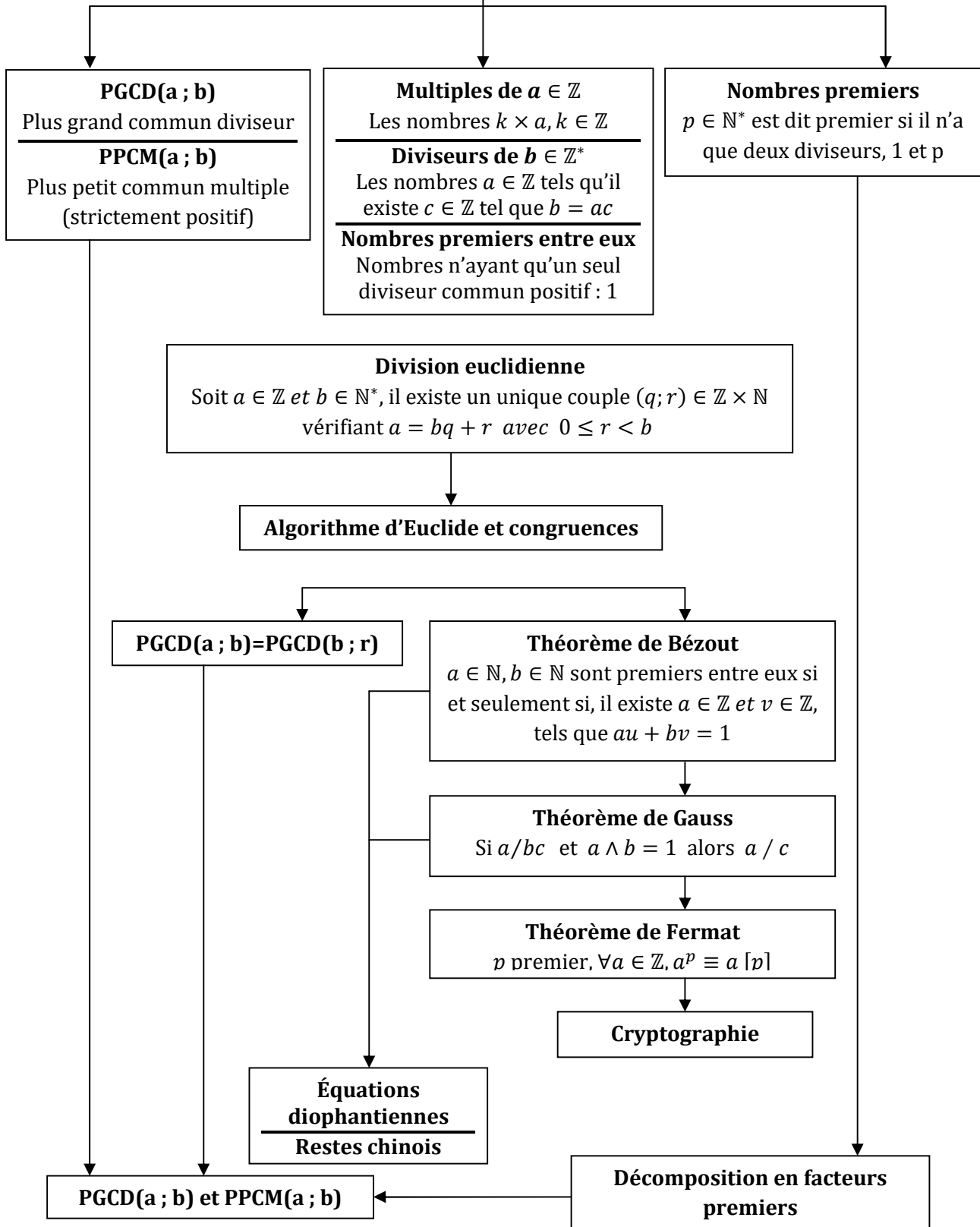
$$N = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 = c_n b^n + c_{n-1} b^{n-1} + \dots + c_1 b + c_0,$$

avec $a_n \times c_n \neq 0$ et $0 \leq a_i, c_i \leq b - 1$, alors $a_i = c_i$ pour tout i . Vu le caractère d'unicité du reste de la division euclidienne de N par b , on a : $a_0 = c_0$. On arrive ensuite à la conclusion en procédant par récurrence finie sur les indices des coefficients.

Déclinaisons des théorèmes d'Arithmétique

Les ensembles de nombres : $\mathbb{N}$ et $\mathbb{Z}$

Le vocabulaire



Bibliographie

Oui, c'est fini... ou presque fini ! Attention, c'est important ! il reste encore la bibliographie. En effet, c'est quoi un livre de mathématiques ou de sciences physiques ou de ... sans sa bibliographie, si ce n'est qu'un leurre ou un manque d'honnêteté intellectuelle autrement dit un délit de plagiat dont l'auteur se cache honteusement derrière sa propre ombre !?

Lors de la rédaction de ce livre, plusieurs manuels et sites ont été consultés (nous exprimons ici notre entière reconnaissance à l'égard de leurs auteurs) :

Bibliographie

- P.H. Terracher-R.Ferachoglou, Maths Term. S Obl. Et spéc. Hachette 2002. ISBN 2.01.13.5294.0
- P.H. Terracher-R.Ferachoglou, Maths Term. S spéc. Hachette 1994. ISBN 2.01.13.4986.9
- J.M. Barros et Col., Maths Term. S spec. Transmath-Nathan 2012. N° édit. 10183118
- J.P. Bouvier, Maths Term. S spec. Belin 1998. ISBN 2.7011.2140.X
- A. Mohsen-S. Nabhout, Géom-Arithm-Prob. MCG Liban 1995. Dépôt légal 03/310409 - 06/627265
- G. Cohen, 52 nouvelles énigmes math. FFJM-vol. 21. Editions POLE 2000. ISBN 2.909737.55.1
- M. Bourahim et col., Ex. corrigés Term Maths Tome 1, MEGAMath 2004. Dépôt légal 2004/2172
- A.S. Haghani et Col., S'exercer en math pour l'examen. Al jadida 2003. Dépôt légal 2003/498
- A.S. Haghani et Col., Alg-Géom-Prob. Ex. Corr. Term SM. Al jadida 1998. Dépôt légal 2003/1576
- A. Mimouni et Col., Maths 4^{ème} année. Kounouz Editions 2014
- S. Touré, Maths Term. SM, CIAM-EDICEF 1999. ISBN 2.84.129554.0
- A. Levine, Maths pour matheux Term. C. Ellipses 1993. ISBN 2.7298.9302.4
- J.L. Boursin, 750 ex. Corr. Term. S. Vuibert 1997. ISBN 2.7117.1413.6
- X. Merlinet B. Clément, Maths Term. S. Ellipses 2012. ISBN 978.2.7298.7623.4
- Iaaly Abdul Raouf, Math. Term. S. Dar-Al Moustakbal 1996 - Tripoli - Liban
- Barache et Bauer, Maths Term. S. 100% Exos. Hatier 2012. ISBN 978.2.218.96268.4
- J.P. Galandrin et Col. Maths Term. S. Spéc. Déclic-Hachette 1998. ISBN 2.01.13.5056.5
- M. Nouvet, Maths Term. S. spéc. Radial-Belin 2006. ISBN 2.7011.4266.0
- R. Cuzel et Col. Algèbre et Prob. Term. D. Delagrave 1967. Dépôt légal : imp.8087 - Edit.3486

Cybergraphie

- | | |
|---|---|
| ➤ http : //www.laroche.free.fr | ➤ https://sites.google.com/site/lapotheme |
| ➤ http://www.mathematiquesfaciles.com | ➤ http://www.lyc-les-iscles.ac-aix-marseille.fr |
| ➤ http://www.recreomath | ➤ http://vivienfrederic.free.fr |
| ➤ http://www.algor.chez.com | ➤ http://mphilippe.fr |
| ➤ http://especesdemaths | ➤ http://www.mathmaurer.com |
| ➤ http://www.mathmoufid.com | ➤ http://autres-talents.fr |
| ➤ http://www.matheleve.net | ➤ http://mathe.kreins |
| ➤ http://www.memopage.com | ➤ https://fr.wikipedia |
| ➤ http://mp.cpgedupuydelome.fr | ➤ http://casemath.free.fr |
| ➤ http://www.lyceedadultes.fr | ➤ http://www.jeusetetmaths.com |
| ➤ http://mathprepa.fr | ➤ http://chingatome.net |
| ➤ http://www.animath.fr | ➤ http://www.lyc-perier.ac-aix-marseille.fr |
| ➤ http://ww2.ac-poitiers.fr | ➤ http://www.lesreferences.com |
| ➤ http://math.seguy.fr | ➤ http://www.bac-de-maths.fr |
| ➤ http://algolycee.free.fr | ➤ http://formation.cepec.free.fr |

Que Dieu me pardonne, si j'ai oublié !

**Eh oui, maintenant, on
peut bien dire que
c'est vraiment fini...**

لَا تُحَرِّمُوا عَلَى الْفُقَرَاءِ مَا حَرَّمَ اللَّهُ وَرَسُولُهُ