Terminale Option Experte/Annales sur le PGCD

1. PGCD, propriété et congruence : *(+2 exercices pour les enseignants)*

Exercice 1

1. a. Montrer que $3n^3-11n+48$ est divisible par $n+3$ pour tout entier naturel n.

   b. Montrer que $3n^2-9n+16$ est un entier naturel non nul pour tout entier naturel n.

2. Montrer que, pour tous les entiers naturels non nuls a, b et c, l'égalité suivante est vraie :
   $\text{pgcd}(a\,;b) = \text{pgcd}(b{\cdot}c{-}a\,;b)$

3. Montrer que, pour tout entier naturel n, supérieur ou égal à 2, l'égalité est vraie :
   $\text{pgcd}\big(3n^3-11n\,;n+3\big)=\text{pgcd}\big(48\,;n+3\big)$

4. a. Détermienr l'ensemble des diviseurs entiers naturels de 48.

   b. En déduire l'ensemble des entiers naturels n tels que $\dfrac{3n^3-11n}{n+3}$ soit un entier naturel.

Exercice 2

On considère la suite (u_n) d'entiers naturels définie par :

$$\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6 \quad \text{pour tout entier naturel } n \end{cases}$$

1. Calculer u_1, u_2, u_3 et u_4.
   Quelle conjecture peut-on émettre concernant les deux derniers chiffres de 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 $n\in\mathbb{N}$: $2{\cdot}u_n = 5^{n+2}+3$.

   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.

Exercice 3

Partie A

On admet que 1 999 est un entier premier. Déterminer l'ensemble des couples $(a\,;b)$ d'entiers naturels admettant pour somme 11 994 et pour $PGCD$ 1 999.

Partie B

On considère l'équation (E) d'inconnu n appartenant à $\mathbb{N}$:

$(E) : n^2-S{\cdot}n+11\,994=0$ où S est un entier naturel.

On s'intéresse à des valeurs de S telle 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 11 994.
   En déduire toutes les valeurs possibles de S telles que (E) admette deux solutions entières.

Partie C

Comment montrerait-on que 1 999 est un entier 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	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97

2. Théorème de Bezout :

Exercice 4

Dans cet exercice, a et b désignent des entiers strictement positifs.

1. a. Démontrer que s'il existe deux entiers relatifs u et v tels que $a{\cdot}u+b{\cdot}v=1$ alors les entiers a et b sont premiers entre eux.

   b. En déduire que si $\big(a^2+a{\cdot}b-b^2\big)^2=1$, alors a et b sont premiers entre eux.

2. On se propose de déterminer les couples d'entiers strictement positifs $(a\,;b)$ tels que $\big(a^2+a{\cdot}b-b^2\big)^2=1$. 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 entiers entiers strictement positifs $(a_n)_n$ définie par $a_0=a_1=1$ et pour tout entier n, $n\geqslant 0$:
$a_{n+2}=a_{n+1}+a_n$.
Démontrer que pour tout entier $n\geqslant 0$, $(a_n\,;a_{n+1})$ est solution.
En déduire que les entiers a_n et a_{n+1} sont premiers entre eux.

Exercice 5

1. Montrer que, pour tout entier naturel non nul k et pour tout entier naturel x :

$$(x-1)\cdot\big(1+x+x^2+\cdots+x^{k-1}\big)=x^k-1$$

Dans toute la suite de l'exercice, on consière 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 :
$n=d\cdot k$
Montrer que a^d-1 est un diviseur de a^n-1.

b. Déduire de la question précédente que $2^{2004}-1$ est divisible par 7, par 63 puis par 9.

3. Soient m et n deux entiers naturels non nuls et d leur *pgcd*.

a. On définit m' et n' par $m=d\cdot m'$ et $n=d\cdot n'$. En appliquant le théorème de Bezout à m' et n', montrer qu'il existe des entiers relatifs u et v tels que :
$m\cdot u-n\cdot v=d$.

b. On suppose u et v strictement positifs.
Montrer que : $\big(a^{m\cdot u}-1\big)-\big(a^{n\cdot v}-1\big)\cdot a^d=a^d-1$
Montrer ensuite que a^d-1 est le *pgcd* de :
$a^{m\cdot u}-1$ et $a^{n\cdot v}-1$

c. Calculer, en utilisant le résultat précédent le *pgcd* de :
$2^{63}-1$ et $2^{60}-1$

3. Théorème de Gauss :

Exercice 6

Soit (E) l'ensemble des entiers naturels écrits, en base 10, sous la forme $\overline{abba}$ où a est un chiffre supérieur ou égal à 2 et b est un chiffre quelconque.
Exemples d'éléments de (E) : 2002 ; 3773 ; 9119.

Nombre d'éléments de (E) ayant 11 comme plus petit facteur premier

1. a. Décomposer 1001 en produit de facteurs premiers.

b. Montrer que tout élément de (E) est divisible par 11.

2. a. Quel est le nombre d'éléments de (E)?

b. Quel est le nombre d'éléments de (E) qui ne sont ni divisibles par 2 ni par 5?

3. soit n un élément de (E) s'écrivant sous la forme $\overline{abba}$.

a. Montrer que :
"*n est divisible par 3 équivaut à $a+b$ est divisible par 3*"

b. Montrer que :
"*n est divisible par 7 équivaut à b est divisible par 7*"

4. Déduire des questions précédentes le nombre d'éléments de (E) qui admettent 11 comme plus petit facteur premier.

Exercice 7

Soit A l'ensemble des entiers naturels de l'intervalle $[1\,;46]$.

1. On considère l'équation : (E) : $23\cdot x+47\cdot y=1$

où x et y sont des entiers relatifs.

a. Donner une solution particulière $\big(x_0\,;y_0\big)$ de (E).

b. Déterminer l'ensemble des couples $(x\,;y)$ solutions de (E).

c. En déduire qu'il existe un unique entier x appartenant à A tel que :
$23\cdot x\equiv 1 \pmod{47}$

2. Soient a et b deux entiers relatifs.

a. Montrer que si $a\cdot b\equiv 0 \pmod{47}$ alors :
$a\equiv 0 \pmod{47}$ ou $b\equiv 0 \pmod{47}$

b. En déduire que si $a^2\equiv 1 \pmod{47}$ alors :
$a\equiv 1 \pmod{47}$; $a\equiv -1 \pmod{47}$

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 $inv(p)$, appartenant à A tel que :
$p\times inv(p)\equiv 1 \pmod{47}$

Par exemple :

- $inv(1)=1$ car $1\times 1\equiv 1 \pmod{47}$
- $inv(2)=24$ car $2\times 24\equiv 1 \pmod{47}$
- $inv(3)=16$ car $3\times 16\equiv 1 \pmod{47}$

b. Quels sont les entiers p de A qui vérifient :
$p=inv(p)$

c. Montrer que : $46!\equiv -1 \pmod{47}$

4. Equation diophantienne :

(+3 exercices pour les enseignants)

Exercice 8

On rappelle que 2 003 est un entier premier.

1. a. Déterminer deux entiers relatifs u et v tels que : $123u + 2003v = 1$

   b. En déduire un entier relatif k_0 tel que : $123k_0 \equiv 1 \pmod{2003}$

   c. Montrer que, pour tout entier relatif x, $123x \equiv 456 \pmod{2003}$ si, et seulement si, $x \equiv 456k_0 \pmod{2003}$

   d. Montrer qu'il existe un unique entier n tel que : $1 \leqslant n \leqslant 2002$ et $123n \equiv 456 \pmod{2003}$

2. Soit a un entier tel que : $1 \leqslant a \leqslant 2002$

   a. Déterminer : $\text{pgcd}(a\,;2003)$

   En déduire qu'il existe un entier m tel que : $a \cdot m \equiv 1 \pmod{2003}$

   b. Montrer que, pour tout entier b, il existe un unique entier x tel que : $0 \leqslant x \leqslant 2\,002$; $a \cdot x \equiv b \pmod{2003}$

Exercice 9

Les parties **A** et **B** sont indépendantes.

Partie A

On considère l'équation (E) : $7x - 6y = 1$ où x et y sont des entiers naturels.

1. Donner une solution particulière de l'équation (E).

2. Déterminer l'ensemble des couples d'entiers naturels solutions de l'équation (E).

Partie B

Dans cette partie, on se propose de déterminer les couples $(n\,;m)$ d'entiers naturels non nul vérifiant la relation :
$$7^n - 3\times 2^m = 1 \quad (F)$$

1. On suppose $m \leqslant 4$.
   Montrer qu'il y a exactement deux couples solutions.

2. On suppose maintenant que $m \geqslant 5$.

   a. Montrer que si le couple $(n\,;m)$ vérifie la relation (F) alors : $7^n \equiv 1 \pmod{32}$

   b. En étudiant les restes de la division par 32 des puissances de 7, montrer que si le couple $(n\,;m)$ vérifie la relation (F) alors n est divisible par 4.

   c. En déduire que si le couple $(n\,;m)$ vérifie la relation (F) alors : $7^n \equiv 1 \pmod{5}$.

   d. Pour $m \geqslant 5$, existe-t-il des couples $(n\,;m)$ d'entiers naturels vérifiant la relation (F)?

3. Conclure, c'est-à-dire déterminer l'ensemble des couples d'entiers naturels non nuls vérifiant la relation (F).

Exercice 10

Les questions 1. et 2. sont indépendantes.

Soit n un entier naturel non nul.

1. On considère l'équation notée (E) :
   $3x + 7y = 10^{2n}$ où x et y sont des entiers relatifs.

   a. Déterminer un couple $(u\,;v)$ d'entiers relatifs tels que : $3 \cdot u + 7 \cdot v = 1$
   En déduire une solution particulière $(x_0\,;y_0)$ de l'équation (E).

   b. Déterminer l'ensemble des couples d'entiers relatifs $(x\,;y)$ solutions de (E).

2. On considère l'équation notée (G) :
   $3x^2 + 7y^2 = 10^{2n}$ où x et y sont des entiers relatifs.

   a. Montrer que : $100 \equiv 2 \pmod{7}$.
   Démontrer que si $(x\,;y)$ est solution de (G) alors : $3x^2 \equiv 2^n \pmod{7}$.

   b. Reproduire et compléter le tableau suivant :

Reste de la division euclidienne de x par 7	0	1	2	3	4	5	6
Reste de la division euclidienne de $3x^2$ par 7							

   c. Démontrer que 2^n est congru à 1, 2 ou 4 modulo 7.
   En déduire que l'équation (G) n'admet pas de solution.

Exercice 11

Partie A - Restitution organisée des connaissances

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 seuleemnt si, il existe un couple $(u\,;v)$ d'entiers relatifs vérifiant $a \cdot u + b \cdot v = 1$.

Théorème de Gauss :
Soient a, b, c des entiers relatifs.
Si a divise le produit $b \cdot c$ 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 $a \equiv 0 \pmod{p}$ et $a \equiv 0 \pmod{q}$, alors $a \equiv 0 \pmod{pq}$

Partie B

On se propose de déterminer l'ensemble $\mathcal{S}$ des entiers relatifs n vérifiant le système :
$$\begin{cases} n \equiv 9 \pmod{17} \\ n \equiv 3 \pmod{5} \end{cases}$$

1. Recherche d'un élément de $\mathcal{S}$.
   On désigne par $(u\,;v)$ un couple d'entiers relatifs tels que : $17 \cdot u + 5 \cdot v = 1$

   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 $\mathcal{S}$.

c. Donner un exemple d'entier n_0 appartenant à $\mathcal{S}$.

2. Caractérisation des éléments de $\mathcal{S}$.

a. Soit n un entier relatif appartenant à $\mathcal{S}$.
Démontrer que : $n-n_0 \equiv 0 \pmod{85}$.

b. En déduire qu'un entier relatif n appartient à $\mathcal{S}$ si, et seulement, si il peut s'écrire sous la forme $n=43+85k$ où k est un entier relatif.

3. Application.
Zoé 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?

5. Problème de codage :

(+1 exercice pour les enseignants)

Exercice 12

Partie A : Restitution organisée de connaissance

Soit a, b, c, d des entiers relatifs et n un entier naturel non nul.

Montrer que si $a \equiv b \pmod{n}$ et si $c \equiv d \pmod{n}$ alors $ac \equiv bd \pmod{n}$.

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 :
$0 \leqslant a \leqslant 25 \quad ; \quad 23a \equiv 1 \pmod{26}$

Partie C : Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

- **Etape 1** Chaque lettre du mot est remplacé 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.

- **Etape 2** $(x_1\,;x_2)$ est transformé en $(y_1\,;y_2)$ tel que :
$$(\mathcal{S}_1) : \begin{cases} y_1 \equiv 11x_1+3x_2 \pmod{26} \\ y_2 \equiv 7x_1+4x_2 \pmod{26} \end{cases}$$
avec $0 \leqslant y_1 \leqslant 25$ et $0 \leqslant y_2 \leqslant 25$

- **Etape 3** $(y_1\,;y_2)$ est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple :
$$\underbrace{\text{TE}}_{\text{mot en clair}} \xrightarrow{\text{étape 1}} (19\,;4) \xrightarrow{\text{étape 2}} (13\,;19) \xrightarrow{\text{étape 3}} \underbrace{\text{NT}}_{\text{mot codé}}$$

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 $(\mathcal{S}_1)$, vérifie les équations du système :
$$(\mathcal{S}_2) : \begin{cases} 23x_1 \equiv 4y_1+23y_2 \pmod{26} \\ 23x_2 \equiv 19y_1+11y_2 \pmod{26} \end{cases}$$

b. A l'aide de la partie **B**, montrer que tout couple $(x_1\,;x_2)$ vérifiant les équations du système $(\mathcal{S}_2)$, vérifie les équations du système :
$$(\mathcal{S}_3) : \begin{cases} x_1 \equiv 16y_1+y_2 \pmod{26} \\ x_2 \equiv 11y_1+5y_2 \pmod{26} \end{cases}$$

c. Montrer que tout couple $(x_1\,;x_2)$ vérifiant les équations du système $(\mathcal{S}_3)$, vérifie les équations du système $(\mathcal{S}_1)$.

d. Décoder le mot YJ

6. Arithmétique et géométrie :

Exercice 13

1. a. Soit p un entier naturel. Montrer que l'un des trois entiers p, $p+10$ et $p+20$, et un seulement est divisible par 3.

b. Les entiers naturels a, b et c sont dans cet ordre les trois premiers terme d'une suite arithmétique de raison 10. Déterminer ces trois entiers sachant qu'ils sont premiers.

2. Soit E l'ensemble des triplets d'entiers relatifs $(u\,;v\,;w)$ tels que :
$$3\cdot u+13\cdot v+23\cdot w=0$$

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 $0 \leqslant r \leqslant 2$.
Montrer que les éléments de E sont de la forme :
$$\big(-13k-23k'-12r \;;\; 3k+r \;;\; 3k'+r\big)$$

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.

Exercice 14

Soit a et b deux entiers naturels non nuls ; on appelle "*réseau*" associé aux entiers a et b l'ensemble des points du plan, muni d'un repère orthonormé, dont les coordonnées $(x\,;y)$ sont des entiers vérifiant les conditions : $0 \leqslant x \leqslant a$; $0 \leqslant y \leqslant b$
On note $R_{a,b}$ ce réseau.

Le but de l'exercice est de relier certaines propriétés arithmétiques des entiers x et y à des propriété géométriques des points correspondants du réseau.

A - Représentation graphique de quelques ensemble

Dans cette question, les réponses sont attendues sans explication, sous la forme d'un graphique qui sera dûment complété sur la feuille annexe à rendre avec la copie.
Représenter graphiquement les points $M(x\,;y)$ du réseau $R_{8,8}$ vérifiant :

1. $x \equiv 2 \pmod{3}$ et $y \equiv 1 \pmod{3}$,
sur le graphique 1 de la feuille annexe.

2. $x + y \equiv 1 \pmod{3}$,
sur le graphique 2 de la feuille annexe.

3. $x \equiv y \pmod{3}$,
sur le graphique 3 de la feuille annexe.

B - Résolution d'une équation

On considère l'équation (E) : $7x - 4y = 1$, où les inconnues x et y sont des entiers relatifs.

1. Déterminer un couple d'entiers relatifs $(x_0\,;y_0)$ solution de l'équation (E).

2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

3. Démontrer que l'équation (E) admet une unique solution $(x\,;y)$ pour laquelle le point $M(x\,;y)$ correspondant appartient au réseau $R_{4,7}$.

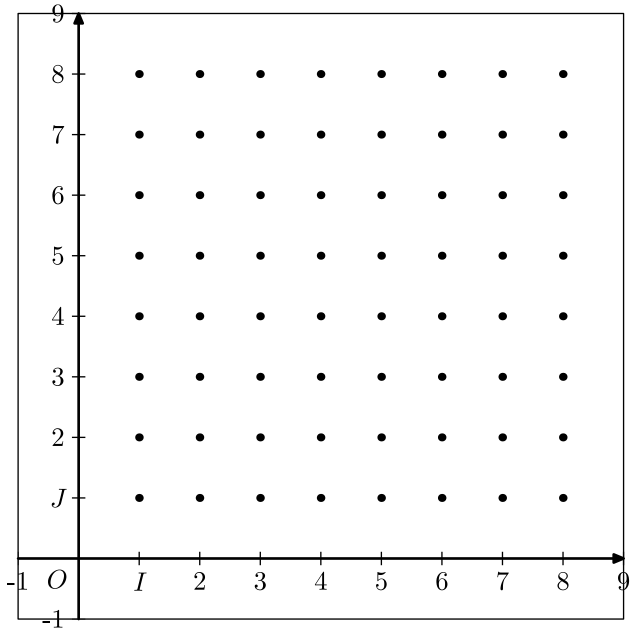
C - Une propriété des points situés sur la diagonale du réseau.

Si a et b sont deux entiers naturels non nuls, on considère la diagonale $[OA]$ du réseau $R_{a,b}$ avec $O(0\,;0)$ et $A(a\,;b)$.

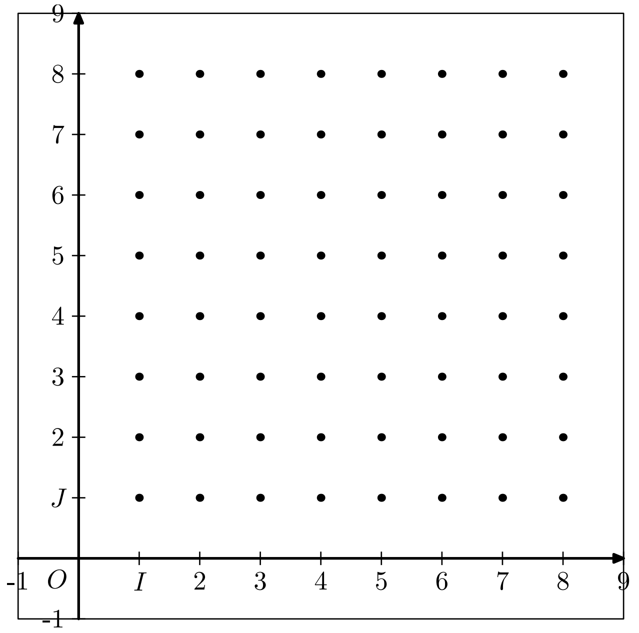
1. Démontrer que les points du segment $[OA]$ sont caractérisés par les conditions :
$0 \leqslant x \leqslant a$; $0 \leqslant y \leqslant b$; $a \cdot y = b \cdot x$

2. Démontrer que si a et b sont premiers entre eux, alors les points O et A sont les seuls points du segment $[OA]$ appartenant au réseau $R_{a,b}$.

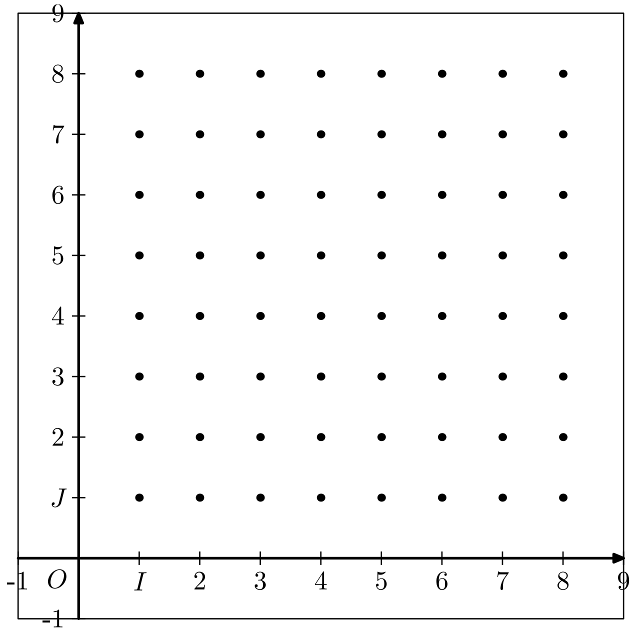
3. Démontrer que si a et b ne sont pas premiers entre eux, alors le segment $[OA]$ contient au moins un autre point du réseau.
(On pourra considérer le pgcd d des entiers a et b et poser $a = d \cdot a'$ et $b = d \cdot b'$)



Graphique 1



Graphique 2



Graphique 3

7. Arithmétique et suite :

(+1 exercice pour les enseignants)

Exercice 15

On considère la suite (u_n) d'entiers naturels définie par :

$$\begin{cases} u_0 = 14 & \\ u_{n+1} = 5u_n - 6 & \text{pour tout entier naturel } n \end{cases}$$

1. Calculer u_1, u_2, u_3 et u_4.
Quelle conjecture peut-on émettre concernant les deux derniers chiffres de 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 $n \in \mathbb{N}$:
$2u_n = 5^{n+2} + 3$.
   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.

Exercice 16

1. Calculer le $PGCD$ de 4^5-1 et de 4^6-1.

Soit u la suite numérique définie par :

$$\begin{cases} u_0 = 0 & \\ u_1 = 1 & \\ u_{n+2} = 5\cdot u_{n+1} - 4\cdot u_n & \text{pour tout entier naturel } n \end{cases}$$

2. Calculer les termes u_2, u_3 et u_4 de la suite u.

3. a. Montrer que la suite u vérifie, pour tout entier naturel n :
$u_{n+1} = 4\cdot u_n + 1$
   b. Montrer que, pour tout entier naturel n, u_n est un entier naturel.
   c. En déduire, pour tout entier naturel n, le $PGCD$ de u_n et u_{n+1}.

4. Soit v la suite définie pour tout entier anturel n par :
$v_n = u_n + \frac{1}{3}$
   a. Montrer que v est une suite géométrique dont on déterminera la raison et le premier terme v_0.
   b. Exprimer v_n puis u_n en fonction de n.
   c. Déterminer, pour tout entier naturel n, le $PGCD$ de $4^{n+1}-1$ et de 4^n-1.

9. Exercices non-classés :

(+4 exercices pour les enseignants)

Exercice 17

Pour chacune des cinq propositions suivantes, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie. Une réponse non démontrée ne rapporte aucun point,

Proposition 1 : Pour tout entier naturel n, 3 divise le nombre entier $2^{2n} - 1$

Proposition 2 : Si un entier relatif x est solution de l'équation $x^2+x \equiv 0 \pmod{6}$ alors $x \equiv 0 \pmod{3}$

Proposition 3 : L'ensemble des couples d'entiers relatifs $(x\,;y)$ solutions de l'équation $12\cdot x - 5\cdot y = 3$ est l'ensemble des couples $(4+10\cdot k\,;9+24\cdot k)$ où $k \in \mathbb{Z}$

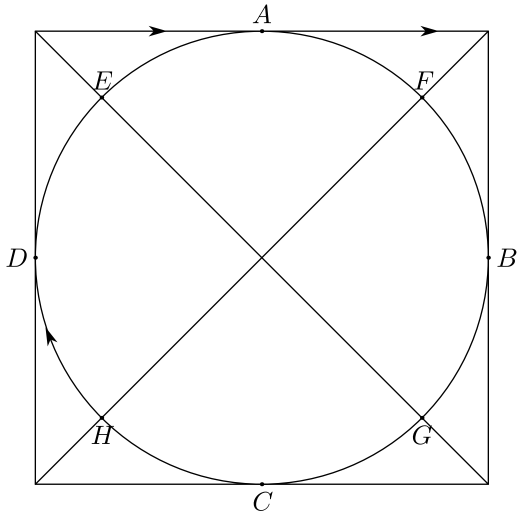
Proposition 4 : Il existe un seul couple $(a\,;b)$ de nombres entiers naturels, tel que :
$a < b$ et $PPCM(a\,;b) - PGCD(a\,;b) = 1$

Deux entiers naturesl M et N sont tels que M a pour écriture abc en base dix et N a pour écriture bca en base dix.
Proposition 5 : Si l'entier M est divisible par 27 alors l'entier $M-N$ est aussi divisible par 27.

Exercice 18

1. On considère l'équation : $(\mathcal{E})$: $17x - 24y = 9$
où $(x\,;y)$ est un couple d'entiers relatifs.
   a. Vérifier que le couple $(9\,;6)$ est solution de l'équation $(\mathcal{E})$.
   b. Résoudre l'équation $(\mathcal{E})$.

2. Dans une fête foraine, Jean s'installe dans un manège circulaire représenté par le schéma de l'annexe 2. Il peut s'installer sur l'un des huits 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 la 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.
A 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. A 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 $(\mathcal{E})$ 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 19

Partie A

Le but de cette partie est de démonstrer que l'ensemble des entiers premiers est infini en raisonnant par l'absurde.

1. On suppose qu'il existe un nombre fini d'entiers premiers notés p_1, p_2, …, p_n.
On considère l'entier E produit de tous les entiers premiers augmenté de 1 :
$E = p_1 \times p_2 \times \cdots \times p_n + 1$
Démontrer que E est un entier supérieur ou égal à 2, et que E est premier avec chacun des entiers p_1, p_2, …, p_n.

2. En utilisant le fait que E admet un diviseur premier, conclure.

Partie B

Pour tout entier naturel $k \geqslant 2$, on pose : $M_k = 2^k - 1$.
On dit que 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									

b. D'après le tableau précédent, si k est un entier premier, peut-on conjecturer que l'entier M_k est premier?

2. Soient p et q deux entiers naturels non nuls.

a. Justifier l'égalité :
$$1 + 2^p + \left(2^p\right)^2 + \cdots + \left(2^p\right)^{q-1} = \frac{\left(2^p\right)^q - 1}{2^p - 1}$$

b. En déduire que $2^{p \cdot q} - 1$ 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 naturel 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 l'entier M_n est premier si, et seulement si, $u_{n-2} \equiv 0 \pmod{M_n}$.
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. La fonction de l'algorithme suivant prend pour argument un entier `n` supérieur ou égal à 3 et doit renvoyer 1 si le nombre de Mersenne M_n est premier et 0 sinon, en utilisant le test de Lucas-Lehmer.

```
Fonction f(n)
    u ← 4
    M ← ...
    Pour i allant de 1 à ...
        u ← ...
    Fin Pour
    Si M divise u
        Alors
            Renvoyer ......
        Sinon
            Renvoyer ......
    Fin Si
```

Recopier et compléter le code de la fonction `f`de façon à ce qu'il remplisse la condition voulue.

Exercice 20

Pour tout entier naturel n non nul, on appelle $S(n)$ le nombre égal à la somme des diviseurs positifs de n.

1. Vérifier que $S(6) = 12$ et calculer $S(7)$.

2. a. Démontrer que, pour tout entier naturel n supérieur ou égal à 2 : $S(n) \geqslant 1 + n$

b. Quels sont les entiers naturels n tels que $S(n) = 1 + n$?

3. On suppose dans cette question que n s'écrit $p \times q$ où p et q sont des entiers premiers distincts.

a. Démontrer que : $S(n) = (1+p)(1+q)$.

b. On considère la proposition suivante :
"*Pour tous entiers naturels n et m non nuls distincts,* $S(n \times m) = S(n) \times S(m)$"
Cette proposition est-elle vraie ou fausse? Justifier.

4. On suppose dans cette question que l'entier n s'écrit p^k, où p est un entier premier et k un entier entier naturel non nul.

a. Quels sont les diviseurs de n?

(b.) En déduire que : $S(n)=\dfrac{1-p^{k+1}}{1-p}$.

5. On suppose dans cette question que n s'écrit $p^{13}\times q^7$, où p et q sont des entiers premiers distincts.

(a.) Soit m un entier naturel.
Démontrer que m divise n si, et seulement si, il existe deux entiers s et t avec $0\leqslant s\leqslant 13$ et $0\leqslant t\leqslant 7$ tels que $m=p^s\times q^t$.

(b.) Démontrer que : $S(n)=\dfrac{1-p^{14}}{1-p}\times\dfrac{1-q^8}{1-q}$

Exercice 21

Pour tout couple d'entiers relatifs non nuls $(a\,;b)$, on note $\text{pgcd}(a\,;b)$ le plus grand diviseur commun de a et b.
Le plan est muni d'un repère $\left(O\,;\,\vec{i}\,;\,\vec{j}\right)$.

1. Exemple. Soit Δ_1 la droite d'équation : $y=\dfrac{5}{4}\cdot x-\dfrac{2}{3}$

(a.) Montrer que si $(x\,;y)$ est un couple d'entiers relatifs alors l'entier $15\cdot x-12\cdot y$ est divisible par 3.

(b.) Existe-il au moins un point de la droite Δ_1 dont les coordonnées sont deux entiers relatifs? Justifier.

Généralisation :

On considère désormais une droite Δ d'équation :
$y=\dfrac{m}{n}\cdot x-\dfrac{p}{q}$
où m, n, p et q sont des entiers relatifs non nuls tels que :
$\text{pgcd}(m\,;n)=\text{pgcd}(p\,;q)=1$
Ainsi, les coefficients de l'équation (E) sont des fractions irréductibles et on dit que Δ est une droite rationnelle.
Le but de l'exercice est de déterminer une condition nécessaire et suffisante sur m, n, p et q pour qu'une droite rationnelle Δ comporte au moins un point dont les coordonnées sont deux entiers relatifs.

2. On suppose ici que la droite Δ comporte un point de coordonnées $(x_0\,;y_0)$ où x_0 et y_0 sont des entiers relatifs.

(a.) En remarquant que le nombre $n\cdot y_0-m\cdot x_0$ est un entier relatif, démontrer que q divise le produit $n\cdot p$.

(b.) En déduire que q divise n.

3. Réciproquement, on suppose que q divise n, et on souhaite trouver un couple $(x_0\,;\,y_0)$ d'entiers relatifs tels que :
$y_0=\dfrac{m}{n}\cdot x_0-\dfrac{p}{q}$.

(a.) On pose $n=q\cdot r$, où r est un entier relatif non nul. Démontrer qu'on peut trouver deux entiers relatifs u et v tels qe :
$q\cdot r\cdot u-m\cdot v=1$.

(b.) En déduire qu'il existe un couple $(x_0\,;y_0)$ d'entiers relatifs tels que :
$y_0=\dfrac{m}{n}\cdot x_0-\dfrac{p}{q}$

4. Soit Δ la droite d'équation $y=\dfrac{3}{8}\cdot x-\dfrac{7}{4}$. Cette droite possède-t-elle un point dont les coordonnées sont des entiers relatifs? Justifier.

5. On considère la fonction `f` d'un algorithme prenant pour argument les entiers `M`, `N`, `P` et `Q`. De plus, on suppose que les arguments passés lors de l'appel à la fonction `f` vérifie :
$\text{pgcd}(\texttt{M}\,;\texttt{N})=\text{pgcd}(\texttt{P}\,;\texttt{Q})=1$

```
Fonction f(M,N,P,Q)
    Si Q divise N
    Alors
        X ← 0
        Tant que  (M/N·X−P/Q n'est pas entier)
                 et  (−M/N·X−P/Q n'est pas entier)
            X ←  X+1
        Fin Tant que
        Si  M/N·X−P/Q  est entier
        Alors
            Renvoyer (X ; M/N·X−P/Q)
        Sinon
            Renvoyer (−X ; M/N·X−P/Q)
        Fin Si
    Sinon
        Renvoyer "Pas de solution"
    Fin si
```

(a.) Justifier que l'appel à la fonction `f` se termine pour toutes valeurs passées en argument de `M`, `N`, `P`, `Q`, entiers relatifs non nuls vérifiant :
$\text{pgcd}(\texttt{M}\,;\texttt{N})=\text{pgcd}(\texttt{P}\,;\texttt{Q})=1$.

(b.) Que permet-il d'obtenir?

Exercice 22

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 "$\star$" 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 :
  $a\longmapsto 0$; $b\longmapsto 1$; ... ; $z\longmapsto 25$.
  On associe au séparateur "$\star$" le nombre entier 26.

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z	$\star$
14	15	16	17	18	19	20	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 "$\star$" a pour rang 26.

- *Deuxièmement :* à chaque élément x de E, l'application g associe le reste de la division euclidienne 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 :
$s\longmapsto 18$; $g(18)=21$; $21\longmapsto v$.
Donc, la lettre s est remplacée lors du codage par la lettre v.

1. Trouver tous les entiers x de E tel que $g(x)=x$, c'est à

dire invariants par l'application g.
En déduire tous 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 $y \equiv 4x+3 \pmod{27}$ alors $x \equiv 7y+6 \pmod{27}$

En déduire que deux caractères distincts sont codés par deux caractères distincts.

3. Proposer une méthode de décodage.

4. Décoder le mot "vfv".

Exercice 23

Les entiers naturels 1, 11, 111, 1111... sont des rep-units. On appelle ainsi les entiers naturels ne s'écrivant qu'avec des 1.

Pour tout entier naturel p non nul, on note N_p le rep-unit s'écrivant avec p fois le chiffre 1 :

$$N_p = \underbrace{11\ldots1}_{\substack{p \text{ répétitions} \\ \text{du chiffre } 1}} = \sum_{k=0}^{k=p-1} 10^k$$

Dans tout l'exercice, p désigne un entier naturel non-nul.
L'objet de cet exercice est d'étudier quelques propriétés des rep-units.

Partie A : divisibilité des rep-units dans quelques cas particuliers

1. Montrer que N_p n'est divisible ni par 2 ni par 5.

2. Dans cette question, on étudie la divisibilité de N_p par 3.

   a. Prouver que, pour tout entier naturel j :
   $10^j \equiv 1 \pmod{3}$

   b. En déduire que $N_p \equiv p \pmod{3}$.

   c. Déterminer une condition nécessaire et suffisante pour que le rep-unit N_p soit divisible par 3.

3. Dans cette question, on étudie la divisibilité N_p par 7.

   a. Recopier et compléter le tableau des congruences ci-dessous, où a est l'unique entier relatif appartenant à : $\{-3\,;-2\,;-1\,;0\,;1\,;2\,;3\}$ tel que : $10^m \equiv a \pmod{7}$
   On ne demande pas de justification.

m	0	1	2	3	4	5	6
a							

   b. Soit p un entier naturel non nul.
   Montrer que $10^p \equiv 1 \pmod{7}$ si, et seulement si, p est un multiple de 6.
   On pourra utiliser la division euclidienne de p par 6.

   c. Justifier que, pour tout entier naturel p non-nul :
   $$N_p = \frac{10^p - 1}{9}$$

   d. Démontrer que "*7 divise N_p*" est équivalent à "*7 divise $9 \cdot N_p$*".

   e. En déduire que N_p est divisible par 7 si, et seulement si, p est un multiple de 6.

Partie B : un rep-unit strictement supérieur à 1 n'est jamais un carré parfait

1. Soit n un entier naturel supérieur ou égal à 2.
On suppose que l'écriture décimale de n^2 se termine par le chiffre 1, c'est à dire $n^2 \equiv 1 \pmod{10}$

   a. Recopier et compléter le tableau de congruences ci-dessous :

$n \equiv \ldots [10]$	0	1	2	3	4	5	6	7	8	9
$n^2 \equiv \ldots [10]$										

   b. En déduire qu'il existe une entier naturel m tel que :
   $n = 10 \cdot m + 1$ ou $n = 10 \cdot m - 1$

   c. Conclure que : $n^2 \equiv 1 \pmod{20}$

2. Soit p un entier naturel supérieur ou égal à 2.
Quel est le reste de la division euclidienne de N_p par 20?

3. En déduire que, pour p entier naturel supérieur ou égal à 2, le rep-unit N_p n'est pas le carré d'un entier.

Exercice 24

A toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le "*chiffre de RABIN*" est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres distincts p et q. Ce couple de nombres est sa clé privée qu'elle garde secrète.
Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leqslant B \leqslant n-1$.
Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.
Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :
$y \equiv x(x+B) \pmod{n}$ avec $0 \leqslant y \leqslant n$

Dans tout l'exercice, on prend $p=3$, $q=11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot "*NO*" à Alice.

1. Montrer que Bob code la lettre "*N*" avec le nombre 8.

2. Déterminer le nombre qui code la lettre "*O*".

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.
Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :
$x(x+3) \equiv 3 \pmod{33}$ $0 \leqslant x < 26$

1. Montrer que $x \cdot (x+13) \equiv 3 \pmod{33}$ équivaut à :
$(x+23)^2 \equiv 4 \pmod{33}$.

2. a. Montrer que si $(x+23)^2 \equiv 4 \pmod{33}$ alors le système d'équations

$$\left\{\begin{array}{l}(x+23)^2 \equiv 4 \pmod{3} \\ (x+23)^2 \equiv 4 \pmod{11}\end{array}\right. \text{ est vérifié.}$$

b. Réciproquement, montrer que si
$$\left\{\begin{array}{l}(x+23)^2 \equiv 4 \pmod{3} \\ (x+23)^2 \equiv 4 \pmod{11}\end{array}\right.$$
alors $(x+23)^2 \equiv 4 \pmod{33}$

c. En déduire que :
$$x\cdot(x+13) \equiv 3 \pmod{33} \iff \left\{\begin{array}{l}(x+23)^2 \equiv 1 \pmod{3} \\ (x+23)^2 \equiv 4 \pmod{11}\end{array}\right.$$

3. a. Déterminer les nombres entiers naturels a tels que $0 \leqslant a < 3$ et $a^2 \equiv 1 \pmod{3}$

b. Déterminer les nombres entiers naturels b tels que $0 \leqslant b < 11$ et $b^2 \equiv 4 \pmod{11}$

4. a. En déduire que $x\cdot(x+13) \equiv 3 \pmod{33}$ équivaut aux quatres systèmes suivants :

$$\left\{\begin{array}{l}x \equiv 2 \pmod{3} \\ x \equiv 8 \pmod{11}\end{array}\right. \text{ ou } \left\{\begin{array}{l}x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{11}\end{array}\right.$$
$$\text{ou } \left\{\begin{array}{l}x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{11}\end{array}\right. \text{ ou } \left\{\begin{array}{l}x \equiv 0 \pmod{3} \\ x \equiv 8 \pmod{11}\end{array}\right.$$

b. On admet que chacun de ces systèmes admet une unique solution entière x telle que $0 \leqslant x < 33$.
Déterminer, sans justification, chacune de ces solutions.

5. Compléter l'algorithme ci-dessous pour qu'il affiche les quatre solutions trouvées dans la question précédente.

```
Pour...allant de...à...
  Si le reste de la division de...par...est égal à...alors
    Afficher ...
  Fin Si
Fin Pour
```

6. Alice peut-elle connaître la première lettre du message envoyé par Bob?
Le "*chiffre de RABIN*" est-il utilisable pour décode un message lettre par lettre?