TS spé — Exercices sur la division euclidienne

1 Effectuer avec la calculatrice la division euclidienne de :
• 220 065 par 324 • 9 876 543 210 par 123 456 789 • 9 999 999 999 999 par 222 222 222 222.
Rappel : Pour la calculatrice Numworks, on a les fonctions rem(p,q) et quo(p,q) [Boîte à outils, rubrique Arithmétique] qui renvoient respectivement le reste et le quotient de la division euclidienne de deux entiers naturels.

1 Déterminer le reste et le quotient de la division euclidienne de :
a) 3113 par 366 ; b) 223 par 5 ; c) – 7 par 2 ; d) 13 par – 3 ; e) – 4 par 21 ; f) 2378881 par 10.

2 Le reste de la division euclidienne d'un entier relatif n par 12 est 7.
Quel est le reste de la division euclidienne de n par 3 ? par 4 ?
Quel est le reste de la division euclidienne de $-n$ par 12 ?

3 Soit a un entier relatif tel que le reste de la division euclidienne de a par 7 soit égal à 5.
Déterminer le reste de la division euclidienne de $2a$ et de $-3a$ par 7.

4
1°) Étude d'exemples
Choisir 4 entiers relatifs quelconques. Vérifier qu'il existe au moins deux entiers dont la différence est divisible par 3. Recommencer avec 4 autres entiers.

Choisir 5 entiers relatifs quelconques. Vérifier qu'il existe au moins deux entiers dont la différence est divisible par 4. Recommencer avec 5 autres entiers.

Le but de la suite de l'exercice est de démontrer la propriété suivante que l'on vient de vérifier dans les uelues cas particuliers précédents.

> Soit p un entier naturel supérieur ou égal à 1.
> Soit E un sous-ensemble de $\mathbb{Z}$ de cardinal strictement supérieur à p.
> Démontrer qu'il existe au moins deux éléments de E dont la différence est un multiple de p.

L'ensemble E peut être fini ou infini.

2°) Démontrer le lemme suivant.
Soit a et b deux entiers relatifs et n un entier relatif non nul.
Si a et b ont le même reste dans leur division euclidienne par n, alors $a-b$ est divisible par n.

Indication : On pourra appliquer le « principe des tiroirs » de Dirichlet.

> Si on doit ranger plus de chaussettes que l'on a de tiroirs, alors l'un des tiroirs contiendra au moins deux chaussettes.

Question : Peut on mathématiser le principe de Dirichlet ? Autrement dit, peut-on donner un énoncé qui ne fasse pas appel à des chaussettes et à des tiroirs ?

> Johann Peter Gustav Lejeune Dirichlet (1805, Düren - 1859, Göttingen) est un mathématicien prussien qui apporta de profondes contributions à la théorie des nombres, en créant le domaine de la théorie analytique des nombres et à la théorie des séries de Fourier. On lui doit d'autres avancées en analyse mathématique. On lui attribue la définition formelle moderne d'une fonction.

3°) À l'aide du lemme, démontrer la propriété de l'encadré.

5 Soit a un entier relatif et b un entier naturel non nul. Soit k un entier naturel quelconque non nul.
On note respectivement q et r le quotient et le reste de la division euclidienne de a par b.
Déterminer le quotient et le reste de la division euclidienne de ka par kb.

6 Déterminer deux entiers naturels x et y sachant que leur somme est égale à 59 et que dans la division euclidienne de x par y le quotient est 8 et le reste 5.

7 Déterminer deux entiers naturels x et y sachant que leur différence est égale à 59 et que dans la division euclidienne de x par y le quotient est 10 et le reste 5.

8 Déterminer tous les entiers naturels n qui, dans la division euclidienne par 7, donnent un quotient égal au reste.
On raisonnera en deux parties :
1ère partie : recherche des valeurs possibles de n ;
2e partie : vérification.
Rédiger une conclusion claire.

9 Dans cet exercice, on s'intéresse au reste de la division euclidienne de $7n+15$ par $3n+2$ pour $n \in \mathbb{N}$.

1°) Remplir un tableau selon le modèle suivant pour les valeurs de n comprises entre 0 et 11.

n	$7n+15$	$3n+2$	reste de la division euclidienne de $7n+15$ par $3n+2$
0			
1			
2			
3			
⋮			
11			

On pourra éventuellement utiliser la calculatrice.

> **Aide pour la calculatrice Numworks :**
>
> On va dans la rubrique Fonctions (ou éventuellement dans la rubrique Suites).
> On tape : $f(x) = \text{rem}(7x+15, 3x+2)$.
> Pour accéder à la fonction rem, ouvrir la Boîte à outils puis aller dans Arithmétique.
> On fait en sorte d'obtenir un tableau de valeurs avec un pas de 1.

À l'aide du tableau, conjecturer une expression du reste en fonction de n, à partir d'un entier naturel n_0 que l'on précisera.

On rédigera une phrase sur le modèle suivant :
D'après la calculatrice, on peut conjecturer que pour $n \geqslant$ ....., le reste de la division euclidienne de $7n+15$ par $3n+2$ est égal à ……. .
2°) Démontrer cette conjecture en utilisant une égalité.
On ne demande pas d'étudier le cas des entiers naturels n strictement inférieurs à n_0.

10 Dans la division euclidienne de 321 par un entier naturel $b \neq 0$, le reste est 75.
Déterminer les valeurs possibles de b et du quotient.

11 Le quotient de la division euclidienne de 1517 par un entier naturel $b \neq 0$ est 75.
Déterminer la valeur de b et du reste.

12 Déterminer les entiers naturels dont la division euclidienne par 43 donne un reste égal au carré du quotient.

13 Démontrer que pour tout entier relatif n, $n(n+2)(n+4)$ est divisible par 3.

Indications :

• Utiliser la propriété du cours :

Tout entier relatif n s'écrit sous la forme $3k$, $3k+1$ ou $3k+2$ avec $k \in \mathbb{Z}$.

• Raisonner ensuite par disjonction de cas (en envisageant 3 cas).

14 1°) Démontrer que, si a et b sont des entiers naturels tels que a^2+b^2 est impair, alors a et b sont de parité différente.
2°) Démontrer qu'un entier naturel impair qui s'écrit comme somme de deux carrés* est de la forme $4K+1$ avec K entier naturel.
3°) En déduire qu'un entier naturel de la forme $4k+3$ avec k entier naturel ne peut pas être la somme de deux carrés.

* Dans cet exercice, le mot « carré » est employé au sens de « carré parfait » c'est-à-dire carré d'un entier naturel.

15 On note q et r respectivement le quotient et le reste de la division euclidienne d'un entier relatif a par un entier relatif b non nul.
Déterminer q sachant que q et r ne changent pas lorsqu'on augmente a de 52 et b de 4.
Indication : Écrire des égalités qui découlent des informations.

16 On fait correspondre à chaque lettre de l'alphabet un entier naturel comme l'indiquent les tableaux 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 définit un système de codage :
- à chaque lettre de l'alphabet, on associe l'entier x correspondant, on associe ensuite à x l'entier y qui est le reste de la division euclidienne de $15x+7$ par 26,
- on associe à y la lettre correspondante.
Ainsi, par cette méthode, la lettre E est associée à 4, 4 est transformé en 15 et 15 correspond à la lettre P et donc la lettre E est codée par la lettre P.

Coder le mot MATHS.

17 Le code INSEE, en France, est un code identifiant chaque individu, utilisé par l'Institut national de la statistique et des études économiques (INSEE), pour différentes analyses statistiques. Ce code s'appelle également NIR (numéro d'inscription au répertoire) et se retrouve sur les cartes de sécurité sociale (carte Vitale par exemple).
Dès la naissance, en France, chaque personne est identifiée par un numéro composé de quinze chiffres. C'est le numéro INSEE ou Numéro de Sécurité Sociale.
Afin d'éviter des erreurs lors des enregistrements (par exemple, lors des remboursements de la Sécurité Sociale), le nombre formé par les deux derniers chiffres est une clé de contrôle.

Exemple :

1	60	04	25	311	114		26
							clé
				matricule			

On considère le nombre formé des treize premiers chiffres. Ce nombre est alors divisé par 97 (division euclidienne). Puis le reste obtenu est soustrait à 97 (97 – reste). Le résultat est la clé de contrôle (écrite avec deux chiffres).

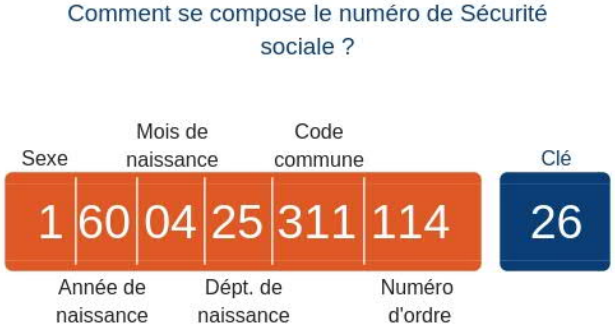
Calculer la clé de contrôle du numéro INSEE tel que le nombre formé des treize premiers chiffres est : 1540250025005.
On pourra :
- soit poser la division euclidienne « à la main » ;
- soit utiliser la calculatrice avec la fonction donnant le reste d'une division euclidienne.

Schéma :

1540250025005
↓ division euclidienne par 97
reste (entre 0 et 96)

clé = 97 – reste (entre 1 et 97)

Vérifier avec son propre numéro de sécurité sociale (présent sur la Carte Vitale).



Idem pour les numéros d'identité bancaire
TS spé Devoir maison lycée Évariste Galois enregistré le 29 décembre 2022
Le R.I.B. (relevé d'identité bancaire) comporte de gauche à droite 5 chiffres pour le code de la banque, 5 chiffres pour le code du guichet, 11 chiffres pour le numéro du compte, 2 chiffres pour la clé K, ainsi calculée : si A est le nombre à 21 chiffres, et si r est le reste de la division euclidienne de 100 A par 97, alors K = 97 – r.
1) Vérifier votre propre clé R.I.B. (ou celle de vos parents).

18 Chiffrement de Hill

Le but de l'exercice est d'étudier une méthode de chiffrement publiée en 1929 par le mathématicien et cryptologue américain Lester Hill. C'est un chiffrement polygraphique, c'est-à-dire qu'on ne (dé)chiffre pas les lettres les unes après les autres, mais par paquets. Nous étudierons la version bigraphique, c'est-à-dire que nous grouperons les lettres deux par deux, mais on peut imaginer des paquets plus grands.

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 y_1 est le reste de la division euclidienne de $11x_1 + 3x_2$ par 26 et y_2 est le reste de la division euclidienne $7x_1 + 4x_2$ par 26.

Étape 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 :

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

Coder le mot ST en détaillant les étapes.

Autre présentation du procédé de chiffrement de Hill avec des matrices :

On donne la matrice $A = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$ (matrice carrée d'ordre 2).

Cette matrice est appelée la clef du chiffrage de Hill.

Le mot à coder est remplacé par la matrice colonne $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, où x_1 est l'entier représentant la première lettre du mot et x_2 l'entier représentant la deuxième, selon le tableau de correspondance qui a été donné auparavant.

• La matrice X est transformée en la matrice colonne $Z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ telle que $Z = AX$.

• La matrice Z est transformée en la matrice $Y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, où y_1 est le reste de la division euclidienne de z_1 par 26 et y_2 le reste de la division euclidienne de z_2 par 26.

• Les entiers y_1 et y_2 donnent les lettres du mot codé, selon le tableau de correspondance qui a été donné.

19 Générateur d'entiers pseudo-aléatoires

On considère la suite (u_n) d'entiers naturels définie sur $\mathbb{N}$ par son premier terme $u_0 = 100$ et u_{n+1} = reste de la division euclidienne de $15091 \times u_n$ par 64007 pour tout entier naturel $n \geqslant 1$.
Rentrer la suite (u_n) dans la calculatrice [indication pour la calculatrice Numworks : $u_{n+1} = \text{rem}(15091u_n, 64007)$].

Cette suite fournit des entiers pseudo-aléatoires entre 0 et 64006.
Les nombres 15091 et 64007 sont des nombres premiers (pour vérifier cela sur la calculatrice Numworks, cliquer sur les trois petits points et demander la décomposition en facteurs premiers).

Que valent u_{30}, u_{300}, u_{3000} ?
Recommencer en prenant d'autres valeurs de u_0.

20 Théorème des dix milieux

Dans le plan P muni d'un repère $(O, \vec{i}, \vec{j})$, on choisit cinq points à coordonnées entières. On a alors dix couples de points ce qui définit dix milieux.
Le but de l'exercice est de démontrer que, quels que soient les cinq points de départ, un milieu au moins a des coordonnées entières.
On note E l'ensemble des points de P dont les deux coordonnées sont des entiers relatifs.
On note :
- E_1 le sous-ensemble de E constitué des points d'abscisse et d'ordonnée paires ;
- E_2 le sous-ensemble de E constitué des points d'abscisse paire et d'ordonnée impaire ;
- E_3 le sous-ensemble de E constitué des points d'abscisse impaire et d'ordonnée paire ;
- E_4 le sous-ensemble de E constitué des points d'abscisse et d'ordonnée impaires.

• Expliquer pourquoi E_1, E_2, E_3, E_4 constituent une partition de E.

• Vérifier que pour tout couple de points de l'un de ces quatre sous-ensembles le milieu appartient à E.

• Conclure en utilisant le principe des tiroirs de Dirichlet vu dans l'exercice **4** .

Corrigé

1 **Division euclidienne de « grands » nombres à l'aide de la calculatrice**

$220\ 065 = 324 \times 679 + 69$

$9876543210 = 12456789 \times 80 + 90$

$9\ 999\ 999\ 999\ 999 = 222\ 222\ 222\ 222 \times 45 + 9$

Rajouter un exercice pour commencer avec des divisions euclidiennes : division euclidienne de 37 par …, de – 507 par …, 25 par 10 …

1

On peut utiliser la calculatrice Numworks.
Exemple : division euclidienne de 3113 par 366

On tape $\frac{3113}{366}$ … résultats complémentaires
Ou

Boîte à outils puis rubrique Arithmétique.

a) $3113 = 366 \times 8 + 185$
Le couple $(\text{quotient} ; \text{reste})$ de la division euclidienne de 3113 par 366 est $(8 ; 185)$.

b) $223 = 5 \times 44 + 3$
Le couple $(\text{quotient} ; \text{reste})$ de la division euclidienne de 223 par 5 est $(44 ; 3)$.
On peut adopter la même présentation qu'à l'école primaire.

c) $-7 = 2 \times (-4) + 1$
Le couple $(\text{quotient} ; \text{reste})$ de la division euclidienne de – 7 par 2 est $(-4 ; 1)$.

Dans notre cas (division euclidienne d'un entier négatif par un entier positif), on observe que le quotient est négatif et par suite, reste > quotient.

On peut calculer $\frac{-7}{2} = -3,5$.
On prend ensuite la partie entière.

d) $13 = (-3) \times (-4) + 1$
Le couple $(\text{quotient} ; \text{reste})$ de la division euclidienne de 13 par – 3 est $(-4 ; 1)$.

e) $-4 = 21 \times (-1) + 17$
Le couple $(\text{quotient} ; \text{reste})$ de la division euclidienne de – 4 par 21 est $(-1 ; 17)$.

Il faut veiller à bien présenter toutes les lettres introduites qui ne sont pas présentées dans l'énoncé.

Exemples :

« Soit *q* le quotient de la division euclidienne de … par … . »

« Soit *r* le reste de la division euclidienne de … par … . »

Attention, il n'est pas toujours utile d'introduire de nouvelles lettres.

Le 28 novembre 2022

T exp Exercices sur la division euclidienne

1

Numworks

$\frac{3113}{366}$ … résultats complémentaires

ou boîte à outils Arithmétique

$223 = 5 \times \underbrace{44} + \underbrace{55}$
quotient reste

$-4 = 21 \times \left(\underbrace{-1}\right) + \underbrace{17}$
quotient reste

reste > quotient

2

Soit *q* le quotient de la division euclidienne de *n* par 12.
On a $n = 12q + 7$ (1).
On travaille avec cette égalité pour faire apparaître les différents restes et quotients demandés.

2

On commence par écrire l'égalité de la division euclidienne de n par 12.

Soit q le quotient de la division euclidienne de n par 12.

Comme le reste de cette division euclidienne est 7, on $n = 12q + 7 \quad (1)$.

> On travaille avec cette égalité pour faire apparaître les différents restes et quotients demandés.

On va travailler avec cette égalité pour répondre aux deux questions.

• (1) s'écrit aussi $n = 3 \times 4q + 7 \quad (1')$.

Toutefois, on ne peut pas en déduire que le reste de la division euclidienne de n par 3 est 7 puisque $7 \geqslant 3$.
Mais $7 = 3 \times 2 + 1$.
$(1')$ permet d'écrire $n = 3 \times 4q + 3 \times 2 + 1 = 3(4q + 2) + 1 \quad (1'')$.

Cette fois, on obtient bien l'égalité traduisant la division euclidienne de n par 3 : le reste est 1 puisque $1 < 3$ et le quotient est $4q + 2$ qui est bien un entier puisque q l'est.

Le reste de la division euclidienne de n par 3 est donc 1.

• On applique la même méthode pour déterminer le reste de la division euclidienne de n par 4.
$n = 4 \times 3q + 7 = 4 \times 3q + 4 \times 1 + 3 = 4(3q + 1) + 3$

Le reste de la division euclidienne de n par 4 est donc 3.

• On reprend l'égalité (1). On multiplie les deux membres par – 1.
$-n = -12q - 7$
Il ne s'agit pas d'une égalité de division euclidienne puisque – 7 est négatif et un reste de division euclidienne ne peut pas être négatif.

On ajoute 12 et on retranche 12. Autrement dit on ajoute $12 - 12$ au membre de droite.

$-n = -12q - 12 + 5$
$-n = 12(-q - 1) + 5$

$-q - 1$ est un entier relatif.
On a donc bien écrit une égalité de division euclidienne.

Le reste de la division euclidienne de $-n$ par 12 est 5 (et le quotient $-q - 1$).

3

On note q le quotient de la division euclidienne de a par 7.

On a $a = 7q + 5$.

$2a = 14q + 10$

$= 14q + 7 + 3$

$= 7(2q + 1) + 3$

Comme q est un entier relatif, $2q + 1$ est un entier relatif.
Le reste de la division euclidienne de $2a$ par 7 est égal à 3.

$-3a = -21q - 15$
$= -21q - 3 \times 7 + 6$
$= -7(3q + 3) + 6$
$= 7(-3q - 3) + 6$

Comme q est un entier relatif, $-3q - 3$ est un entier relatif.
Le reste de la division euclidienne $-3a$ par 7 est égal 6.

4

On note :
r le reste des divisions euclidiennes de a et b par n (on sait par hypothèse que les deux divisions donnent le même reste).
q et q' les quotients respectifs de ces deux divisions.
On a $r < |n|$.
On écrit les égalités de divisions euclidiennes : $a = nq + r$ et $b = nq' + r$.
On calcule alors $a - b$.

$a - b = (nq + r) - (nq' + r) = n(q - q')$

Or q et q' sont des entiers relatifs donc $q - q'$ est un entier relatif.
On en déduit que $a - b$ est un multiple de n.

Application :

On suppose que $E \subset \mathbb{Z}$ et que card $E > p$.

Démontrer qu'il existe au moins deux éléments de E dont la différence est un multiple de p.

Les valeurs possibles du reste de la division euclidienne d'un entier relatif n par p sont 0, 1, …, $p - 1$. Il y a donc p restes possibles.

Comme card $E > p$, d'après le principe de Dirichlet, il existe au moins deux éléments de E qui ont le même reste dans la division euclidienne par p.

D'après le résultat démontré dans l'exercice, leur différence (peu importe l'ordre) est un multiple de p.

Exemple :
Si on a 12 entiers relatifs deux à deux distincts, il en existe au moins deux dont la différence est un multiple de 11.

5

On a : $a = bq + r$ et $r < b$.

En multipliant les deux membres de l'égalité par *k*, on obtient l'égalité $ka = q \times kb + kr$.

Or $r < b$. Donc en multipliant les deux membres de l'inégalité par k $(k > 0)$, $kr < kb$.

De plus, *q* est un entier relatif et *kr* est un entier naturel (ce que l'on peut écrire $(q\,;kr) \in \mathbb{Z} \times \mathbb{N}$).

D'après ce qui précède, on peut affirmer que la division euclidienne de *ka* par *kb* donne un quotient égal à *q* et un reste égal à *kr*.

6

$x = 53$ et $y = 6$

Solution détaillée :

Déterminons deux entiers naturels *x* et *y* sachant que leur somme est égale à 59 et que dans la division euclidienne de *x* par *y* le quotient est 8 et le reste 5.

On rappelle tout d'abord le théorème de la division euclidienne dans $\mathbb{N}$:

Pour tout couple $(a\,;b)$ d'entiers naturels, avec $b \neq 0$, il existe un unique couple $(q\,;r)$ d'entiers naturels tels que $a = bq + r$ et $r < b$.

Il n'est pas obligatoire de l'écrire dans la version au propre.

x et *y* vérifient le système (I) $\begin{cases} x + y = 59 \\ x = y \times 8 + 5 \end{cases}$ avec la condition $5 < y$.

Il faut dire que $5 < y$ (condition de la division euclidienne).

(I) est un système linéaire de deux équations à deux inconnues.

On peut utiliser plusieurs méthodes de résolution :
- résolution par substitutions
- résolution par combinaisons (combinaisons linéaires)
- résolution matricielle
- résolution à la calculatrice

On présente deux méthodes de résolution par substitution.

$$\text{(I)} \Leftrightarrow \begin{cases} y = 59 - x \\ x = (59 - x) \times 8 + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 59 - x \\ x = 472 - 8x + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 59 - x \\ 9x = 477 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 59 - x \\ x = \dfrac{477}{9} \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 59 - 53 \\ x = 53 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 6 \\ x = 53 \end{cases}$$

$$\text{(I)} \Leftrightarrow \begin{cases} 8y + 5 + y = 59 \\ x = 8y + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} 9y + 5 = 59 \\ x = 8y + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} 9y = 54 \\ x = 8y + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = \dfrac{54}{9} \\ x = 8y + 5 \end{cases}$$

$$\Leftrightarrow \begin{cases} y = 6 \\ x = 53 \end{cases}$$

$$\boxed{\begin{cases} x = 53 \\ y = 6 \end{cases}}$$

On a $5 < 6$.
On peut donc valider $x = 53$ et $y = 6$.

Texte surligné en jaune ci-dessous à enlever
On a : $53 = 6 \times 8 + 5$ et $5 < 6$.
Cette égalité traduit donc la division euclidienne de *x* par *y*.

On peut donc valider $x = 53$ et $y = 6$.

Autre façon :

x	y
5	8

On a donc $\begin{cases} x = 8y + 5 & (1) \\ x + y = 59 & (2) \end{cases}$.

Avec (1), (2) donne $8y + 5 + y = 59$ (2').

(2') $\Leftrightarrow 9y = 54$

$\Leftrightarrow y = 6$

On obtient alors $x = 8 \times 6 + 5$
$= 53$

Donc le couple cherché est le couple $(53\,;6)$.

7

$x=65$ et $y=6$

Solution détaillée :

Déterminons deux entiers naturels x et y sachant que leur différence est égale à 59 et que dans la division euclidienne de x par y le quotient est 10 et le reste 5.

Comme le quotient de la division euclidienne de x par y est égal à 10 donc non nul, on a : $x \geqslant y$ (et même $x > y$).

En effet, d'après le cours, lorsque x et y sont deux entiers naturels tels que $x < y$, le quotient de la division euclidienne de x par y est égal à 0 (puisque l'on écrit $x = y\times 0 + x$).

x et y vérifient le système (I) $\begin{cases} x-y=59 \\ x=y\times 10+5 \end{cases}$ avec $5<y$ (condition de la division euclidienne).

(I) $\Leftrightarrow \begin{cases} y=x-59 \\ x=10y+5 \end{cases}$

$\Leftrightarrow \begin{cases} y=x-59 \\ x=10(x-59)+5 \end{cases}$

$\Leftrightarrow \begin{cases} y=x-59 \\ x=10x-590+5 \end{cases}$

$\Leftrightarrow \begin{cases} y=x-59 \\ x=10x-585 \end{cases}$

$\Leftrightarrow \begin{cases} y=x-59 \\ x=10x-585 \end{cases}$

$\Leftrightarrow \begin{cases} y=x-59 \\ -9x=-585 \end{cases}$

$\Leftrightarrow \begin{cases} y=6 \\ x=65 \end{cases}$

$\Leftrightarrow \begin{cases} x=65 \\ y=6 \end{cases}$

On a $5<6$.
On peut donc valider $x=53$ et $y=6$.

On a : $65=10\times 6+5$ et $5<6$.
Cette égalité traduit donc la division euclidienne de x par y.

On peut donc valider $x=65$ et $y=6$.

Autre façon :

x	y
5	10

On a donc $\begin{cases} x=10y+5 & (1) \\ x-y=59 & (2) \end{cases}$.

Avec (1), (2) donne $10y+5-y=59$ (2').

(2') $\Leftrightarrow 9y=54$
$\Leftrightarrow y=6$

On obtient alors $x-6=59$
$=65$

Donc le couple cherché est le couple (65 ; 6).

8

Déterminons tous les entiers naturels qui, dans la division euclidienne par 7, donnent un quotient égal au reste.

On va raisonne en deux parties.

1ère partie :

Soit n un entier naturel tel que le quotient et le reste dans la division euclidienne de n par 7 soient égaux.

Notons q et r respectivement le quotient et le reste de la division euclidienne de n par 7.
On a $q\in\mathbb{N}$ et $r\in\mathbb{N}$.

L'égalité de la division euclidienne de n par 7 s'écrit : $n=7q+r$ avec $0\leqslant r<7$ (1).

Comme $q=r$, on a alors $n=7q+q$ d'où $n=8q$.

Or comme $q=r$, (1) donne $q\in\{0\,;1\,;2\,;3\,;4\,;5\,;6\}$.

2e partie :

On examine une par une les valeurs de q obtenues dans la 1ère partie.

On peut faire un tableau de valeurs.

q	n	Égalité de division euclidienne
0	0	$0=0\times7+0$
1	8	$8=1\times7+1$
2	16	$16=2\times7+2$
3	24	$24=3\times7+3$
4	32	$32=4\times7+4$
5	40	$40=5\times7+5$
6	48	$48=6\times7+6$

Conclusion :
Les valeurs de *n* cherchées sont 0, 8, 16, 24, 32, 40, 48.
ou
Les entiers naturels *n* cherchés sont tous les multiples de 8 compris entre 0 et 48.

Autre façon :

$n=7r+r$
$n=8r$
etc.

9

On s'intéresse au reste de la division euclidienne de $7n+15$ par $3n+2$ pour $n\in\mathbb{N}$.

Cette division euclidienne est possible car $7n+15$ et $3n+2$ sont des entiers et $\forall n\in\mathbb{N}\quad 3n+2\neq 0$ (le diviseur est non nul).

1°)

n	$7n+15$	$3n+2$	reste de la division euclidienne de $7n+15$ par $3n+2$
0	15	2	1
1	22	5	2
2	29	8	5
3	36	11	3
4	43	14	1
5	50	17	16
6	57	20	17
7	64	23	18
8	71	26	19
9	78	29	20
10	85	32	21
11	92	35	22

Il peut être intéressant de rajouter une colonne avec les quotients.
Cela peut aider pour la recherche de la solution.

n	$7n+15$	$3n+2$	quotient de la division euclidienne de $7n+15$ par $3n+2$	reste de la division euclidienne de $7n+15$ par $3n+2$
0	15	2	7	1
1	22	5	4	2
2	29	8	3	5
3	36	11	3	3
4	43	14	3	1
5	50	17	2	16
6	57	20	2	17
7	64	23	2	18
8	71	26	2	19
9	78	29	2	20
10	85	32	2	21
11	92	35	2	22

Conjecturons le reste de la division euclidienne de $7n+15$ par $3n+2$ avec $n\in\mathbb{N}$ à partir d'un entier naturel n_0.

Avec la calculatrice, on trouve une formule. Cette formule ne « marche » pas pour $n<n_0$.

On rédige ainsi :

D'après la calculatrice,
Grâce au tableau,

on peut conjecturer que pour tout entier naturel $n\geqslant 5$, le reste de la division euclidienne de $7n+15$ par $3n+2$ est égal à $n+11$.

On cherche une expression explicite du reste en fonction de *n*.

2°) **Démontrons la conjecture émise au 1°).**

On se base sur l'égalité de la division euclidienne d'un entier naturel *a* par un entier naturel *b* non nul :

$a=bq+r$ avec $0\leqslant r<b$ [à ne pas écrire dans la version au propre du corrigé].

• On ne peut pas (ou du moins pas très facilement) démontrer le résultat en faisant une démonstration par récurrence.

• On démontre directement le résultat en travaillant avec des égalités.

• On travaille en littéral.

Pour tout entier naturel n, on a : $7n+15=2(3n+2)+n+11$.

Cette égalité est valable pour tout entier naturel n.
Pour que cette égalité traduise une division euclidienne, il faut que deux conditions soient vérifiées.

Condition C_1 : 2 et $n+11$ sont des entiers naturels.

Condition C_2 : On doit avoir $n+11<3n+2$ (1).

Dans cette inégalité, le « strictement inférieur » est fondamental.

$(1) \Leftrightarrow n>\frac{9}{2}$

$\Leftrightarrow n \geqslant 5$ (puisque n est un entier naturel)

Bilan :

Dans le cas où $n \geqslant 5$, nous pouvons donc dire que le reste de la division euclidienne de $7n+15$ par $3n+2$ est $n+11$.

On a déterminé la division euclidienne de $7n+15$ par $3n+2$ lorsque $n \geqslant 5$ (on a le quotient et le reste).
On ne doit regarder les cas où $n<5$ car l'énoncé dit que l'on s'intéresse juste aux cas $n \geqslant 5$.

Le 31 octobre 2016

La disposition traditionnelle (avec signe de potence) ne marche pas pour ce type d'exercice, ni pour les négatifs.

10

On sait que le reste de la division euclidienne de 321 par l'entier naturel $b \neq 0$ est 75.
Déterminons les valeurs possibles de b et du quotient.

Notons q le quotient de la division euclidienne de 321 par b.

On sait que $q \in \mathbb{N}$.

On a donc $321=b\times q+75$ (1) avec la condition $b>75$ (condition sur le reste dans une division euclidienne).

(1) donne $b\times q=246$ $(1')$.

$(1')$ exprime que b et q sont des diviseurs associés positifs de 246.

On cherche toutes les possibilités d'écrire 246 comme produit de deux entiers naturels.

On trouve 4 égalités :
$246=1\times 246$
$246=2\times 123$
$246=3\times 82$
$246=6\times 41$

Pour trouver les diviseurs positifs de 246, plutôt que de faire une recherche « à la main » (qui prend un petit peu de temps), on peut utiliser un programme sur calculatrice (voir « Algorithmes liés à la divisibilité et à la division euclidienne »).

On doit avoir $b>75$ (condition écrite ci-dessus). On ne retient donc pas la dernière égalité.

Les couples (b, q) cherchés sont $(246,1)$, $(123,2)$ et $(82,3)$.

11

Le quotient de la division euclidienne de 1517 par l'entier naturel $b \neq 0$ est 75.
Déterminons la valeur de b et du reste.

Par hypothèse, $b \in \mathbb{N}^*$.

Soit r le reste de la division euclidienne de 1517 par b.

L'égalité de la division euclidienne de 1517 par b s'écrit $1517=b\times 75+r$ (1) avec la condition $0 \leqslant r<b$ (2).

(1) donne $r=1517-75b$.

L'inégalité (2) permet alors d'écrire $0 \leqslant 1517-75b<b$.

Cette inégalité donne alors $b \leqslant \frac{1517}{75}$ et $b>\frac{1517}{76}$ autrement dit $\frac{1517}{76}<b \leqslant \frac{1517}{75}$.
Or $\frac{1517}{75}=20,22...$ et $\frac{1517}{76}=19,96...$.

Donc comme $b \in \mathbb{N}^*$, $b = 20$.

On en déduit que $r = 1517 - 75 \times 20 = 17$.

Conclusion : $b = 20$ et $r = 17$

Autre façon :

1517	b
r	75

D'où $1517 = 75b + r$ avec $1517 > b > r$.

Autre méthode :

$1517 = 75 \times 20 + 17$

Conclusion : $b = 20$ et $r = 17$.
C'est un coup de « bol » !

Exemple : $20 = 2 \times 7 + 6$. Cette égalité exprime la division euclidienne de 20 par 7 mais elle n'exprime pas la division euclidienne de 20 par 2.

12

Déterminons les entiers naturels dont la division euclidienne par 43 donne un reste égal au carré du quotient.

Meilleure version qui sera détaillée lors de la correction en classe en 2018-2019 :

a vérifie la condition $(C) \Leftrightarrow$ il existe $q \in \mathbb{N}$ tel que $a = 43q + q^2$ et $q^2 < 43$.

Raisonnement en deux parties : recherche des entiers naturels possibles et vérification.
Il est possible de raisonner directement par équivalences mais c'est plus compliqué.

1ère partie :

Soit n un entier naturel tel que la division euclidienne de n par 43 donne un reste égal au carré du quotient.

On note :
q le quotient de la division euclidienne de n par 43 ;
r le reste de la division euclidienne de n par 43.

q et r sont des entiers naturels.

On a : $n = 43q + r$ et $0 \leqslant r < 43$.

On peut remarquer également que comme n est positif ou nul, q est positif ou nul.
Cela va avoir un rôle important dans la suite de l'exercice.

De plus, $r = q^2$.
On peut donc écrire $n = 43q + q^2$ (1) et $q^2 < 43$ (2).

(2) donne $q < \sqrt{43}$ (car q est un entier naturel donc est positif ou nul).

Réciproquement :
Soit a un entier naturel qui s'écrit sous la forme $a = 43q + q^2$ (1) où q est un entier naturel vérifiant $q^2 < 43$ (2).
Dans ce cas, l'égalité (1) traduit bien la division euclidienne de a par 43.

On en déduit que les entiers naturels cherchés sont les entiers naturels de la forme $a = 43q + q^2$ (1) où q est un entier naturel vérifiant $q^2 < 43$ (2).
On va donner les différentes de a pour conclure.

On reprend l'inégalité (2).

On connaît la liste des carrés parfaits : $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$…
Les valeurs possibles de q sont donc 0, 1, 2, 3, 4, 5, 6.

Autres méthodes déconseillées :

Grâce à la calculatrice, on trouve $\sqrt{43} = 6,56\ldots$.
On peut aussi écrire, sans calculatrice, que $\sqrt{36} < \sqrt{43} < \sqrt{49}$ donc $6 < \sqrt{43} < 7$.

L'inégalité (2) donne donc $q \leqslant 6$.

Il y a donc 7 valeurs possibles de q.

On calcule alors les différentes valeurs de n en utilisant l'égalité (1) [$n = 43q + q^2$]. On peut effectuer les calculs à la main ou utiliser la calculatrice en rentrant la fonction $x \mapsto 43x + x^2$.

q	n
0	0
1	44
2	90
3	138
4	188
5	240
6	294

Par exemple, pour $q = 1$, $n = 43 \times 1 + 1^2 = 44$.

2e partie : Vérification :
On prend les 7 valeurs possibles de n : 0, 44, 90, 138, 188, 240, 294.
On effectue leur division euclidienne par 43 et on vérifie dans chacun des cas que le reste égal au carré du quotient.

Conclusion :

Les entiers naturels cherchés sont 0, 44, 90, 138, 188, 240 et 294.

Version courte qui montre la structure de l'exercice (mais mal rédigée) :

On cherche entiers naturels n qui s'écrivent sous la forme $n = 43q + q^2 \quad (1)$ où q est un entier naturel vérifiant $q^2 < 43 \quad (2)$.
La condition (2) équivaut à $q \leqslant 6$.

L'égalité (1) fournit donc les valeurs suivantes de n : 44, 90, 138, 188, 240 et 294.

13

Démontrons que pour tout entier relatif n, $n(n+2)(n+4)$ est divisible par 3.

On ne peut pas démontrer ce résultat par récurrence.

On pose $A = n(n+2)(n+4)$ avec $n \in \mathbb{Z}$.

Voir méthode plus rapide un peu plus loin

Phrase à ne pas écrire dans le corrigé au propre : Dans la division euclidienne par 3, il y a 3 restes possibles : 0 ; 1 ; 2. Cette phrase sert juste à rappeler la justification du résultat de cours utilisé dans la suite.

D'après le cours, tout entier relatif n s'écrit sous l'une des formes $3k$; $3k+1$; $3k+2$ (k étant un entier relatif).
Nous avons donc 3 cas à étudier :

• Si $n = 3k$ avec $k \in \mathbb{Z}$, alors $A = 3k(3k+2)(3k+4)$
Donc 3 | A car $k(3k+2)(3k+4)$ est un entier relatif.

• Si $n = 3k+1$ avec $k \in \mathbb{Z}$, alors $A = (3k+1)(3k+1+2)(3k+1+4)$
$= (3k+1)(3k+3)(3k+5)$
$= 3(k+1)(3k+1)(3k+5)$

Or $(k+1)(3k+1)(3k+5) \in \mathbb{Z}$ donc 3| A.

• Si $n = 3k+2$ avec $k \in \mathbb{Z}$, alors $A = (3k+2)(3k+2+2)(3k+2+4)$
$= (3k+2)(3k+4)(3k+6)$
$= 3(k+2)(3k+2)(3k+4)$

Donc 3| A.

Conclusion :

Dans tous les cas, A est divisible par 3 (ou 3|A).

La proposition est donc démontrée pour tout entier naturel n.

On peut aussi adopter la méthode plus rapide suivante.

D'après le cours, tout entier relatif n s'écrit sous l'une des formes $3k$; $3k+1$; $3k+2$ (k étant un entier relatif).

Nous avons donc 3 cas à étudier :

• 1er cas : $n = 3k$ avec $k \in \mathbb{Z}$

On sait qu'alors n est un multiple de 3 donc A est un multiple de 3.

• 2e cas : $n = 3k+1$ avec $k \in \mathbb{Z}$

$n+2 = 3k+1+2 = 3k+3 = 3(k+1)$ donc $n+2$ est un multiple de 3 et par suite, A est un multiple de 3.

• 3e cas : $n = 3k+2$ avec $k \in \mathbb{Z}$

$n+4 = 3k+2+4 = 3k+6 = 3(k+2)$ donc $n+4$ est un multiple de 3 et par suite, A est un multiple de 3.

Dans tous les cas, A est divisible par 3.

14

1°) **Démontrons que, si a et b sont des entiers naturels tels que $a^2 + b^2$ est impair, alors a et b sont de parité différente.**

On rappelle que pour tout entier relatif n, n^2 a la même parité que n.

1ère méthode : rapide et efficace

$a^2 + b^2$ impair $\Leftrightarrow$ a^2 et b^2 sont de parités différentes
$\Leftrightarrow$ a et b sont de parités différentes (car a^2 et b^2 ont les mêmes parités respectives que a et b)

2e méthode : plus longue (donc à éviter)
On raisonne par **disjonction de cas**.

On rappelle que si n est un entier naturel alors n^2 a la même parité.
Donc a^2 et b^2 ont les mêmes parités respectives que a et b.

1er cas : a est pair et b est pair.
Dans ce cas, a^2 est pair et b^2 est pair.
Donc a^2+b^2 est pair.

2e cas : a est pair et b est impair.
Dans ce cas, a^2 est pair et b^2 est impair.
Donc a^2+b^2 est impair.

3e cas : a est impair et b est impair.
Dans ce cas, a^2 est impair et b^2 est impair.
Donc a^2+b^2 est pair.

4e cas : a est impair et b est pair.
Dans ce cas, a^2 est impair et b^2 est pair.
Donc a^2+b^2 est impair.

On en déduit que si a^2+b^2 est impair, alors a et b sont de parité différente.

Une autre façon de faire est de raisonner par **contraposée** c'est-à-dire de démontrer que si a et b sont de même parité, alors a^2+b^2 est pair.

En fait, on vient de démontrer une équivalence.

On s'appuie sur les lemmes de parité suivants qui sont très simples à démontrer :

- La somme de deux entiers pairs est un entier pair.
- La somme de deux entiers impairs et un entier pair.

- Le produit d'un nombre pair par un entier quelconque est un entier pair.
- Le produit de deux entiers impairs est un entier impair.

En fait, on a même démontré une équivalence.
On a démontré l'équivalence suivante :
a^2+b^2 impair $\Leftrightarrow$ a et b de parités différentes

2°) **Démontrons qu'un entier naturel impair qui s'écrit comme somme de deux carrés est de la forme $n=4K+1$ avec $K\in\mathbb{N}$.**

Soit n un entier naturel impair tel que $n=a^2+b^2$ où a et b sont des entiers naturels.

D'après la question 1°), les entiers a et b sont de parité différente.

L'un des deux s'écrit donc sous la forme $2k$; l'autre s'écrit sous la forme $2k'+1$ où k et k' sont des entiers naturels.

On ne peut pas prendre le même k !
On est obligé de prendre deux lettres différentes !

On a alors $n=4k^2+4k'^2+4k+1$.

On peut donc écrire $n=4\left(k^2+k'^2+k'\right)+1$.

Posons $K=k^2+k'^2+k'$.

$K\in\mathbb{N}$ et on a $n=4K+1$ ce qui démontre le résultat.

3°) **Déduisons-en qu'un entier naturel de la forme $4k+3$ avec $k\in\mathbb{Z}$ ne peut pas être la somme de deux carrés.**

Soit n un entier naturel de la forme $4k+3$ avec $k\in\mathbb{N}$.

n est impair car n est la somme de $4k$ qui est pair et de 3 qui est impair.
(on peut aussi dire $n=2(k+1)+1$ donc $n=2k'+1$ en posant $k'=k+1$, avec $k'\in\mathbb{N}$).

Si était la somme de deux carrés, il devrait être de la forme $4K+1$ avec $K\in\mathbb{N}$.

Or n est de la forme $4k+3$ avec $k\in\mathbb{N}$ donc ne peut pas être de la forme $4K+1$ avec $K\in\mathbb{N}$.

On en déduit que n n'est pas la somme de deux carrés.

La recherche des entiers qui peuvent s'écrire comme somme de deux carrés est un problème d'arithmétique très intéressant.

15

$(a\,;b)\in\mathbb{Z}\times\mathbb{Z}^*$
q : quotient de la division euclidienne de a par b
r : reste de la division euclidienne de a par b

Déterminons q sachant que q et r ne changent pas lorsqu'on augmente a de 52 et b de 4.

L'égalité de la division euclidienne de a par b s'écrit $a=bq+r$ (1) avec la condition $0\leqslant r<|b|$.
L'égalité de la division euclidienne de $a+52$ par $b+4$ s'écrit $a+52=(b+4)q+r$ (2) avec la condition $0\leqslant r<|b+4|$.

(2) donne $a+52=bq+4q+r$.
On remplace a par $bq+r$.
On obtient alors $bq+r+52=bq+4q+r$.
D'où $52=4q$.
Donc $q=\dfrac{52}{4}=13$.

16

Dans cet exercice, on étudie un exemple de **codage affine**.

Codons le mot MATHS.

• M est associé à l'entier 12.

$15\times12+7=187$
$187=26\times7+5$
Le reste de la division euclidienne de 187 par 26 est 5.
5 correspond à la lettre F.
La lettre M est donc codée par F.

• A est associé à l'entier 0.

$15\times0+7=7$
$7=26\times0+7$
Le reste de la division euclidienne de 7 par 26 est 7.
7 correspond à la lettre H.
La lettre A est donc codée par H.

• T est associé à l'entier 19.

$15\times19+7=292$
$292=26\times11+6$
Le reste de la division euclidienne de 292 par 26 est 6.
6 correspond à la lettre G.
La lettre T est donc codée par G.

• H est associé à l'entier 7.

$15\times7+7=112$
$112=26\times4+8$
Le reste de la division euclidienne est 8.
8 correspond donc à la lettre I.
La lettre H est codée par I.

• S est associé à l'entier 18.

$15\times18+7=277$
$277=26\times10+17$
Le reste de la division euclidienne de 277 par 26 est 17.
17 correspond à la lettre R.
La lettre S est donc codée par R.

Conclusion : Le mot MATHS est codé par FHGIR.

Pour aller plus vite, on peut utiliser la calculatrice et faire un tableau de correspondance : on utilise la commande de la calculatrice qui permet d'obtenir le reste d'une division euclidienne.

$Y1=\text{remainder}(15X+7,26)$ ou $Y1=\text{reste}(15X+7,26)$

$Y1=15X+7-\text{partEnt}((15X+7)/26)*26$

On obtient le tableau de correspondance suivant (en rouge : chiffres et lettres codés).

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
7	22	11	0	15	4	19	8	25	12	1	16	5
H	W	L	A	P	E	T	I	X	M	B	Q	F

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
20	9	24	13	2	17	6	21	10	25	14	3	18
U	T	Y	N	C	R	G	V	K	Z	O	D	S

D'après le tableau, on peut dire qu'il s'agit d'un « bon » codage. En effet, deux lettres distinctes sont bien codées par deux lettres distinctes.

17

On utilise la calculatrice en ligne fournie par le site calc.name.

$\text{mod}(1540250025005,97)=16$
Le reste de la division euclidienne de 1540250025005 par 97 est 16.

Soustrayons ce reste 16 à 97.

$97-16=81$

Nous obtenons 81. La clé de ce numéro de Sécurité Sociale est 81.

18

Chiffrement de Hill

Étape 1 :

ST correspond à $(x_1\,;x_2)=(18\,;19)$.

Étape 2 :

• $11x_1+3x_2=11\times18+3\times19=198+57=255$
y_1 est alors le reste de la division euclidienne de 255 par 26.
Comme $255=9\times26+21$ et que $0\leqslant21<26$, on en déduit que $y_1=21$.
• $7x_1+4x_2=7\times18+4\times19=126+76=202$. Comme $202=7\times26+20$ et que $0\leqslant20<26$, on en déduit que $y_2=20$.

Étape 3 :

Le couple $(21;20)$ correspond au mot VU et donc le mot ST se code en VU.
Il est possible de créer un petit programme de codage sur calculatrice.

Auguste Charpentier le 1-12-2020 (élève de terminale maths experts)

```
def hill(text):
    result = ""
    for i in range(0, len(text), 2):
        a = text[i]
        b = text[i+1]
        a = letters.index(a)
        b = letters.index(b)
        a = (11*a + 3*b) % 26
        b = (7*a + 4*b) % 26
        result = result + letters[a] + letters[b]
  return result

print(hill("MATH"))
```

Commentaires pour le programme d'Auguste Charpentier notés le 14-12-2020

```
1.  letters = "ABCDEFHIJKLMNOPQRSTUVWXYZ"
2.
3.
4.  def hill(text):
5.      result = ""  # notre futur texte codé
6.
7.      # on rentre dans une itération avec un pas de 2 car on
8.      # travaille avec des paquets de 2 lettres dans le texte.
9.      # len(text) renvoie la longueur du texte, donc 4 avec "MATH"
10.     for i in range(0, len(text), 2):
11.
12.         # on obtient les deux lettres suivantes dans notre texte
13.         a = text[i]
14.         b = text[i + 1]
15.
16.         # première étape : on obtient le nombre correspondant à la
    lettre
17.         a = letters.index(a)
18.         b = letters.index(b)
19.
20.         # deuxième étape : on effectue la division euclidienne
21.         a = (11 * a + 3 * b) % 26
22.         b = (7 * a + 4 * b) % 26
23.
24.         # troisième étape : on réutilise nos lettres pour construire
    le mot, qu'on ajoute à result
25.         result = result + letters[a] + letters[b]
26.
27.     return result
28.
29.
30. print(hill("MATH"))
31. >>> SQJC
```

Dans ce programme, on va progressivement coder notre texte par paquets de 2.

On rentre dans une boucle for allant de 0 à n, la longueur de notre texte, avec un pas de 2.
Si on a un texte de 6 caractères, la boucle sera exécutée 3 fois, avec i valant 0 puis 2 puis 4.

Ensuite, on va obtenir `a` et `b`, les deux lettres avec lesquelles on va travailler.
En faisant `"MATH"[2]`*, on va obtenir* `"T"` *(le compte commençant à 0)*
On va donc aller prendre `text[i]` pour la première lettre `a` et `text[i + 1]` pour la deuxième lettre `b`.

Première étape
On cherche à traduire `a` et `b` en fonction de la position de la lettre dans l'alphabet.

On a `letters` qui est une chaîne de caractères pour tout l'alphabet.
La fonction `index` nous permet de nous donner la position de la première occurrence dans le texte.
`letters.index` donne donc la position d'une lettre de 0 à 26.

On a donc `a` et `b` qui sont égaux à x_1 et x_2.

Deuxième étape

On cherche à traduire a et b selon les divisions euclidiennes, traduites ainsi en Python :

```
1.  a = (11 * a + 3 * b) % 26
2.  b = (7 * a + 4 * b) % 26
```

L'opérateur % correspond au modulo, le reste de la division de a par b.

On a donc a et b qui sont égaux à y_1 et y_2.

Troisième étape
On cherche à traduire a et b pour qu'ils soient égaux à une nouvelle lettre dans l'alphabet.

On effectue la même opération `letters[x]` tel que x est la position de la lettre de 0 à 26 dans l'alphabet.
On additionne nos deux lettres ensemble, puis on les ajoute à `result`.

Enfin, on renvoie `result`.

19

$$(u_n)\begin{cases} u_0 = 100 \\ \forall n \in \mathbb{N}^* \quad u_n = \text{reste de la division euclidienne de } 15091 \times u_{n-1} \end{cases}$$

Que valent u_{30}, u_{300}, u_{3000} ?
42782 (le 2 mars 2023)
35181
36849

Recommencer en prenant d'autres valeurs de u_0.
u_0 s'appelle la « graine ».

```
def al(n):
    u=100
    for i in range(1,n+1):
        u=(15091*u)%64007
    return u
```

La fonction fournit un entier naturel pseudo-aléatoire inférieur ou égal à 64006.

13 Générateur d'entiers pseudo-aléatoires

On considère la suite (u_n) d'entiers naturels définie sur $\mathbb{N}$ par son premier terme $u_0 = 100$ et
$u_n =$ reste de la division euclidienne de $15091 \times u_{n-1}$ par 64007 pour tout entier naturel $n \geqslant 1$.
Programmer le calcul des termes de la suite (u_n) en Python.
Que valent u_{30} ? u_{300} ? u_{3000} ?

$u_{n+1} = \text{rem}(15091.u_n, 64007)$
$u_0 = 100$

$u_{30} = 17988$
$u_{300} = 52175$
$u_{3000} = 57295$

Le choix $u_0 = 0$ est mauvais car on obtient toujours 0.

Il s'agit d'une méthode utilisée en informatique pour obtenir des nombres pseudo-aléatoires pour produire des nombres aléatoires depuis qu'elle a été inventée en 1948 par D. H Lehmer.

Une autre méthode est la méthode des carrés médians de Von Neumann en 1946.

20 Le corrigé sera fait en classe.

Ici, on a choisi cinq points rouges. Alors, forcément deux au moins vont se retrouver dans la même famille (car il y a 5 points et 4 familles, donc pas assez de familles pour que chaque points soit séparé de tous les autres - c'est ce qu'on appelle le principe des tiroirs).
Alors pour ces deux points, comme leurs abscisses x_1 et x_2 sont de même parité, l'abscisse de leur milieu (la moyenne de x_1 et x_2) est un nombre entier. De même, l'ordonnée du milieu est un nombre entier. Et alors ce milieu est exactement sur le quadrillage !
Bien entendu, avec seulement 4 points, il est possible de s'arranger pour avoir tous les milieux hors du quadrillage : il suffit de prendre un point dans chaque famille !