Divisibilité et congruences

1 Divisibilité dans $\mathbb{Z}$

On rappelle que l'ensemble des entiers naturels est noté $\mathbb{N}$ et que l'ensemble des entiers relatifs est noté $\mathbb{Z}$.

Définition 1 : Soit a et b deux entiers relatifs avec $b \neq 0$.

On dit que a **divise** b s'il existe un entier relatif k tel que $b = ka$. On note ceci $a|b$.
On dit également que a est un **diviseur** de b ou que b est un **multiple** de a.

■ **Exemple 1 :** $4 \mid 24$. En effet, $24 = 6 \times 4$. ■

■ **Exemple 2 :** L'ensemble des diviseurs de 8 est $\{-8; -4; -2; -1; 1; 2; 4; 8\}$. ■

■ **Exemple 3 :** Pour tout entier relatif p, on a $p \mid p$, $-p \mid p$, $1 \mid p$ et $-1 \mid p$. ■

■ **Exemple 4 :** Montrons que pour tout entier naturel n, $12n + 7$ n'est pas un multiple de 4.

Nous raisonnerons par **l'absurde** : nous supposerons que le contraire de cette affirmation est vraie et aboutirons à une absurdité. Cela nous permettra de conclure que l'hypothèse de départ n'était pas raisonnable.

Supposons qu'il existe un entier n pour lequel $12n + 7$ est un multiple de 4. Cela signifie qu'il existe un entier k tel que $12n + 7 = 4k$. Mais alors, $7 = 4k - 12 = 4(k - 3)$. On a écrit 7 comme le produit de 4 et d'un entier : 7 serait donc un multiple de 4. C'est absurde ! Notre hypothèse de départ était donc fausse.

Ainsi, pour tout entier naturel n, $12n + 7$ n'est pas un multiple de 4. ■

Propriété 1 : Soit a, b et c trois entiers relatifs, avec a et b non nuls. Si $a \mid b$ et $b \mid c$, alors $a \mid c$. On dit que la relation de divisibilité est **transitive**.

Démonstration 1.1 : Traduisons les hypothèses de l'énoncé

- $a \mid b$: il existe un entier relatif k tel que $b = ka$
- $b \mid c$: il existe un entier relatif k' tel que $c = k'b$

Ainsi, $c = k'b = k' \times ka = (k'k) \times a$. On a écrit c sous la forme d'un entier multiplié par a. c est donc un multiple de a et donc $a \mid c$. □

Propriété 2 : Soit a et b deux entiers relatifs tels que $a \mid b$. Alors tout diviseur de a est un diviseur de b.

■ **Exemple 5 :** On souhaite déterminer si 246 est un diviseur de 7416487.

- D'une part, 246 est pair : on a $2 \mid 246$
- Si $246 \mid 7416487$, alors, d'après la propriété précédente, on aurait également que $2 \mid 7416487$. Ce qui n'est pas le cas.

Ainsi, 246 n'est pas un diviseur de 7416487. ■

Propriété 3 : Soit a, b et c trois entiers relatifs. On suppose que a et b sont des multiples de c.

Alors, pour tous entiers relatifs u et v, $ua+vb$ est un multiple de c.

Démonstration 1.2 : Traduisons le fait que a et b sont des multiples de c.

- Il existe un entier relatif k tel que $a=kc$.
- Il existe un entier relatif k' tel que $b=k'c$.

Ainsi, $ua+vb=ukc+vk'c=(uk+vk')c$.
On a écrit $ua+vb$ sous la forme d'un entier relatif multiplié par c : $ua+vb$ est donc un multiple de c. □

■ **Exemple 6 :** On sait que 21 et 36 sont des multiples de 3. Alors, $17\times 21+147\times 36$ est un multiple de 3.■

■ **Exemple 7 :** Déterminons les entiers relatifs n pour lesquels $n+4$ divise $3n+17$.

Nous procéderons par analyse-synthèse : nous allons d'abord établir une liste de candidats puis nous vérifierons pour chacun de ces candidats s'il convient.

Analyse : Soit n un entier naturel tel que $n+4 \mid 3n+17$. On sait par ailleurs que $n+4 \mid n+4$. Ainsi, $n+4$ divise également $3n+17-3(n+4)$. Or, $3n+17-3(n+4)=3n+17-3n-12=5$. Ainsi, $n+4$ divise 5. Or, les diviseurs de 5 sont -5, -1, 1 et 5. Cela nous laisse 4 possibilités.

- $n+4=-5$ et donc $n=-9$
- $n+4=-1$ et donc $n=-5$
- $n+4=1$ et donc $n=-3$
- $n+4=5$ et donc $n=1$

Synthèse : Il reste à vérifier, parmi les valeurs trouvées, celles qui fonctionnent.

- Si $n=-9$, alors $n+4=-5$ et $3n+17=-10$. On a bien $-5 \mid -10$.
- Si $n=-5$, alors $n+4=-1$ et $3n+17=2$. On a bien $-1 \mid 2$.
- Si $n=-3$, alors $n+4=1$ et $3n+17=8$. On a bien $1 \mid 8$.
- Si $n=1$, alors $n+4=5$ et $3n+17=20$. On a bien $5 \mid 20$.

Les solutions de ce problème sont donc -9, -5, -3 et 1. ■

2 Division euclidienne

Théorème 2.1 — Division euclidienne. : Soit $a\in\mathbb{Z}$ et $b\in\mathbb{N}$, avec $b\neq 0$.

Il existe un **unique** couple d'entiers relatifs $(q;r)$ tel que $a=bq+r$ et $0\leqslant r<b$.

Cette relation s'appelle la division euclidienne de a par b.

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

Démonstration 2.2 — Unicité. : Supposons qu'il existe deux couples d'entiers relatifs $(q;r)$ et $(q';r')$ tels que $a=bq+r=bq'+r'$, avec $0\leqslant r<b$ et $0\leqslant r'<b$

Alors, $bq-bq'=r'-r$ ce qui entraîne que $b(q-q')=r'-r$. Ainsi, b est un diviseur de $r-r'$. Or, $r'-r$ est strictement compris entre $-b$ et b. On a donc $r-r'=0$ et donc $r'=r$.

Ainsi, $b(q-q')=0$, mais puisque b est différent de 0, il en vient que $q-q'=0$ et donc que $q=q'$. □

■ **Exemple 8 :** Prenons $a = 2122$ et $b = 7$. On a alors $2122 = 7 \times 303 + 1$.

- Le quotient de la division euclidienne de 2122 par 7 est 303
- Le reste de cette division euclidienne est 1

■

■ **Exemple 9 :** Prenons $a = 247$ et $b = 6$. On a bien $247 = 6 \times 40 + 7$. Pour autant, il ne s'agit pas de la division euclidienne de 247 par 6 : le reste doit être impérativement inférieur à 6. ■

■ **Exemple 10 :** Soit n un entier naturel. Déterminons le reste de la division euclidienne de $7n + 13$ par $3n + 2$.

D'une part, $7n + 13 = 2 \times (3n + 2) + n + 9$

Il s'agit de la division euclidienne de $7n + 13$ par $3n + 2$ **à condition que le reste soit positif et strictement inférieur au diviseur** !

Puisque pour tout entier naturel n, $n + 9 > 0$, il faut donc que $n + 9 < 3n + 2$, c'est-à-dire $-2n < -7$ et donc $n > \frac{7}{2}$. n étant entier, on a donc $n + 9 < 3n + 2$ à partir de $n = 4$.

Ainsi, si $n \geqslant 4$, le reste de la division euclidienne de $7n + 13$ par $3n + 2$ est $n + 9$. Il faut alors traiter les autres valeurs de n au cas par cas...

n	$7n + 13$	$3n + 2$	Div. Euc.	Reste
0	13	2	$13 = 2 \times 6 + 1$	1
1	20	5	$20 = 5 \times 4 + 0$	0
2	27	8	$27 = 8 \times 3 + 3$	3
3	34	11	$20 = 11 \times 3 + 1$	1

■

Propriété 4 : Soit a un entier relatif et b un entier naturel non nul.

b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration 2.3 : Si le reste de la division euclidienne de a par b est nul, alors il existe un entier relatif q tel que $a = bq$. b divise donc a.

Si b divise a, alors il existe un entier relatif q tel que $a = bq = bq + 0$. Par unicité de la division euclidienne, le reste de la division de a par b vaut 0. □

Propriété 5 : Soit b un entier naturel supérieur ou égal à 2.

Pour tout entier relatif a, il existe un entier relatif q tel que a s'écrit sous l'une des formes suivantes : bq, $bq + 1$, $bq + 2$, ... , $bq + (b - 1)$

■ **Exemple 11 :** Prenons $b = 2$. Tout entier relatif s'écrit sous la forme $2k$ ou $2k + 1$. Les premiers sont les nombres pairs et les seconds sont les nombres impairs. ■

■ **Exemple 12 :** Soit n un entier naturel. Montrons que n^2+1 n'est jamais divisible par 3.

Nous allons faire une **disjonction de cas** : d'après la propriété précédente, n peut s'écrire sous la forme $3k$, $3k+1$ ou $3k+2$. Soit k un entier relatif

- $(3k)^2+1=9k^2+1$. Or, $3|9$ donc $3|9k^2$. Si $9k^2+1$ était divisible par 3, alors $9k^2+1-9k^2$ le serait aussi... Mais cette quantité vaut 1, qui n'est pas divisible par 3. Ainsi, $9k^2+1$ n'est pas un multiple de 3.
- $(3k+1)^2+1=9k^2+6q+2=3(3k^2+2k)$. De la même manière que pour le point précédent, puisque 2 n'est pas divisible par 3, $(3k+1)^2+1$ ne l'est pas non plus.
- $(3k+2)^2+1=9k^2+12k+5=3(3k^2+4k)+5$, qui n'est pas un multiple de 3.

Dans tous les cas, n^2+1 n'est pas un multiple de 3.

■

3 Congruence

3.1 Congruence modulo n

Définition 2 : Soit n un entier naturel non nul, a et b deux entiers relatifs. On dit que a est congrus à b modulo n si a et b ont le même reste dans la division euclidienne par n.

On écrit $a \equiv b\,[n]$

■ **Exemple 13 :** $13 \equiv 21\,[4]$. En effet, la division euclidienne de 21 par 4 est $21=4\times 5+1$ et celle de 13 par 4 est $13=4\times 3+1$. 13 et 21 ont donc pour reste 1 dans la division euclidienne par 4. ■

Cette définition est évidemment motivée par l'existence et l'unicité de la division euclidienne. Plutôt que d'affirmer qu'un entier n peut s'écrire sous une des formes $3k$, $3k+1$ ou $3k+2$, pour k un certain entier, on peut également dire que l'on se trouve dans l'une des situations suivantes : $n\equiv 0\,[3]$, $n\equiv 1\,[3]$ ou $n \equiv 2\,[3]$.

D'une manière plus générale...

Propriété 6 : Soit a un entier relatif et n un entier naturel non nul. Il existe un unique $m\in\{0;1;2;\dots;n\}$ tel que $a\equiv m\,[n]$.

Démonstration 3.1 : Le m en question n'est autre que le reste de la division euclidienne de a par n. □

Il existe toutefois une autre manière, sans doute plus commode de définir les congruences.

Propriété 7 : Soit n un entier naturel non nul, a et b deux entiers relatifs.

Alors $a\equiv b\,[n]$ si et seulement si $(a-b)$ est un multiple de n.

En particulier, a est un multiple de n si et seulement si $a \equiv 0\,[n]$.

Démonstration 3.2 : Soit n un entier naturel non nul, a et b deux entiers relatifs. Écrivons alors la division euclidienne de a et b par n

- Il existe deux entiers relatifs q et r tels que $a=nq+r$ et $0\leqslant r<n$
- Il existe deux entiers relatif q' et r' tels que $b=nq'+r$ et $0\leqslant r'<n$

Nous raisonnerons par double implication

- Supposons que $a\equiv b\,[n]$. On a alors $r=r'$. Ainsi, $(a-b)=nq+r-(nq'+r)=n(q-q')$. $(a-b)$ est donc bien un multiple de n.

- Réciproquement, supposons que $(a-b)$ est un multiple de n. Alors il existe un entier relatif k tel que $a-b=kn$. Or, $a-b=nq+r-nq'-r'=n(q-q')+r-r'$ et donc $kn=n(q-q')+r-r'$ ce qui entraîne $n(k-q+q')=r-r'$. $r-r'$ est donc un multiple de n. Seulement, on a $-n<r-r'<n$. Il en vient que $r-r'=0$ et donc que $r=r'$.

□

■ **Exemple 14 :** On a $414 \equiv 144\,[27]$. En effet, $414-144=270$, qui est un multiple de 27. ■

3.2 Compatibilité de la congruence avec les opérations

Propriété 8 — Relation d'équivalence. : Soit n un entier naturel non nul

- Pour tout entier relatif a, $a \equiv a\,[n]$. La relation de congruence est **réflexive**.
- Pour tous entiers relatifs a et b, si $a \equiv b\,[n]$, alors $b \equiv a\,[n]$. La relation de congruence est **symétrique**.
- Pour tous entiers relatifs a, b et c, si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$. La relation de congruence est **transitive**.

On dit que la relation de congruence modulo n est une relation d'équivalence sur l'ensemble des entiers relatifs.

Démonstration 3.3 :
- On a $a-a=0$, qui est bien un multiple de n.
- Si $a \equiv b\,[n]$, alors il existe un entier relatif k tel que $a-b=kn$ et donc $b-a=(-k)n$. $b-a$ est donc un multiple de n. On a donc $b \equiv a\,[n]$
- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors il existe des entiers relatifs k et k' tels que $a-b=kn$ et $b-c=k'n$. Mais alors, $a-c=a-b+b-c=kn+k'n=(k+k')n$. $a-c$ est donc un multiple de n et donc $a \equiv c\,[n]$

□

Propriété 9 : Soit n un entier naturel non nul, a, b, c et d quatre entiers relatifs

- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors $a+c \equiv b+d\,[n]$.
- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors $ac \equiv bd\,[n]$. En particulier, $a^k \equiv b^k\,[n]$ pour tout entier naturel k.
- Si $a \equiv b\,[n]$, alors pour tout entier relatif m, $ma \equiv mb[mn]$

Démonstration 3.4 :
- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors il existe deux entiers relatifs k et k' tels que $a-b=kn$ et $c-d=k'n$. Ainsi, $a+c-(b+d)=a-b+c-d=kn+k'n=(k+k')n$. Il en vient que $(a+c)-(b-d)$ est un multiple de n. On a donc bien $a+c \equiv b+d\,[n]$.
- Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors il existe deux entiers relatifs k et k' tels que $a-b=kn$ et $c-d=k'n$. On a donc $a=b+kn$ et $c=d+k'n$. Ainsi,

  $$ac-bd=(b+kn)(d+k'n)-bd=bd+bk'n+dkn+kk'n^2-bd=(bk'+dk+kk'n)n$$

  Le passage aux puissances se montre par récurrence en utilisant la propriété que nous venons de démontrer. Ainsi, $ac-bd$ est un multiple de n. On a donc bien $ac \equiv bd\,[n]$.
- Si $a \equiv b\,[n]$, alors il existe un entier relatif k tel que $a-b=kn$. Mais alors $ma-mb=m(a-b)=mkn=k(mn)$, qui est un multiple de mn. On a donc bien $ma \equiv mb[mn]$

□

Les règles opératoires sur les congruences nous permettent de résoudre plus facilement les questions de divisibilité. En effet, dire qu'un nombre est divisible par un autre, c'est dire qu'il est congrus à 0 modulo ce dernier entier.

■ **Exemple 15 :** Montrons que, pour tout entier naturel n, $2^{3n} - 1$ est un multiple de 7. On sait que pour tout entier naturel n, $2^{3n} = (2^3)^n = 8^n$. Or, $8 \equiv 1\,[7]$. Ainsi, pour tout entier naturel n, $2^{3n} - 1 \equiv 1^n - 1 \equiv 0\,[7]$. $2^{3n} - 1$ est donc bien un multiple de 7. ■

Une des applications les plus courantes des congruences est le raisonnement par disjonction de cas.

■ **Exemple 16 :** Soit n un entier naturel. On souhaite déterminer les valeurs de n pour lesquelles $5n^2 + 19n - 2$ est divisible par 4. On raisonne par disjonction de cas, suivant la congruence de n modulo 4. Notons d'abord que, puisque $5 \equiv 1\,[4]$ et $19 \equiv 3\,[4]$, alors $5n^2 + 19n - 3 \equiv n^2 + 3n - 3\,[4]$

$n \equiv \dots\,[4]$	0	1	2	3
$n^2 \equiv \dots\,[4]$	0	1	0	1
$3n \equiv \dots\,[4]$	0	3	2	1
$n^2 + 3n - 3 \equiv \dots\,[4]$	-2	-2	0	0

Ainsi, $5n^2 + 19n - 2$ est divisible par 4 si et seulement si $n \equiv 2\,[4]$ ou $n \equiv 3\,[4]$ (ou encore, s'il existe un entier relatif k tel que $n = 4k + 2$ ou $n = 4k + 3$). ■

Il faut toutefois faire attention lorsque l'on manipule des entiers en exposant. Nous disposons pas - à ce stade - de règles qui permettent de simplifier directement les exposants. Une méthode très utile est d'étudier les puissances d'un nombre jusqu'à tomber sur une congruence à 1. A partir de là, les congruences de toutes les puissances de ce nombre peuvent se déduire très facilement.

■ **Exemple 17 :** On souhaite savoir le reste de la division euclidienne de 8^{483} par 5.

D'abord, remarquons que $8 \equiv 3\,[5]$. On a donc $8^{483} \equiv 3^{483}\,[5]$. En revanche, il n'est pas possible d'appliquer un même raisonnement sur le nombre en exposant. Regardons plutôt les premières puissances de 2...

- On a $3^0 = 1$ et donc $3^0 \equiv 1[5]$. Par ailleurs, $3^1 = 3$ et donc $3^1 \equiv 3\,[5]$
- On a $3^2 = 9$ et donc $3^2 \equiv 4\,[5]$.
- On pourrait alors calculer directement 3^3 et déterminer sa congruence modulo 5... Mais épargnons-nous ce souci ! En effet, puisque $3^2 \equiv 4\,[5]$, en multipliant cette relation par 3, on obtient que $3^3 \equiv 12\,[5]$. Or, $12 \equiv 2\,[5]$. Finalement, $3^3 \equiv 2\,[5]$
- On procède de la même manière pour 3^4 : puisque $3^3 \equiv 2\,[5]$, on a alors $3^4 \equiv 6\,[5]$. Or, $6 \equiv 1\,[5]$. Finalement, $3^4 \equiv 1\,[5]$.
- On pourrait alors continuer ainsi. On trouverait $3^5 \equiv 3\,[5]$, $3^6 \equiv 4\,[5]$, $3^7 \equiv 2\,[5]$ et $3^8 \equiv 1\,[5]$

On remarque alors que les congruences sont cycliques, de période 4... En fait, on peut s'arrêter dès que l'on trouve une puissance de 3 congrus à 1 modulo 5 : il s'agit de 3^4.

Pour savoir à quoi est congrus 3^{483} modulo 5, il suffit donc de savoir à quoi est congrus 483 modulo 4.

Or, $483 = 4 \times 120 + 3$. Ainsi, $3^{483} = 3^{4\times 120+3} = (3^4)^{120} \times 3^3$. Ainsi,

$$8^{483} \equiv 3^{483} \equiv 3^3 \equiv 2\,[5]$$

Le reste de la division euclidienne de 8^{483} par 5 est 2. ■

Exercices

1 Divisibilité dans $\mathbb{Z}$

► Exercice 1
Donner l'ensemble des diviseurs de 18, de 24 et de -31

► Exercice 2
On dit qu'un nombre est parfait s'il est égal à la somme de ses diviseurs positifs stricts. Par exemple, les diviseurs positifs stricts de 6 sont 1, 2 et 3 et $6 = 1 + 2 + 3$. Montrer que 28 est un nombre parfait.

► Exercice 3
Montrer que la somme de trois entiers consécutifs est toujours divisible par 3.

► Exercice 4
Soit n un entier relatif. Montrer que $51n - 12$ n'est pas un multiple de 17.

► Exercice 5
Montrer que si un nombre est un multiple de 24, alors c'est un multiple de 6 et un multiple de 4. La réciproque est-elle vraie ?

► Exercice 6
Dresser la liste des diviseurs de 28 puis déterminer les entiers relatifs n tels que $9n - 5$ divise 28.

► Exercice 7
On considère la fonction f définie pour tout entier relatif n différent de 2 par $f(n) = \dfrac{3n^2 + 5n - 3}{n - 2}$

1. Déterminer les valeurs des réels a, b et c tels que, pour tout entier naturel n différent de 2, on ait
$$f(n) = an + b + \frac{c}{n-2}$$
2. Quelles sont les valeurs de n pour lesquelles l'image par f est un entier ?

► Exercice 8
Soit n un entier naturel. Montrer que $9n^3 + 36n^2 - 21n + 30$ est un multiple de 3.

► Exercice 9
Déterminer l'ensemble des entiers relatifs n tels que $2n + 3$ divise $6n + 8$.

► Exercice 10
Soit a et n deux entiers naturels tels que a divise $3n + 5$ et $7n + 2$

1. Montrer que a divise 29.
2. En déduire les valeurs possibles de a.

► **Exercice 11**
Montrer par récurrence que pour tout entier naturel n, $8^n - 3^n$ est divisible par 5.

► **Exercice 12**
On rappelle que si q est un réel différent de 1 et n un entier naturel non nul, alors

$$1 + q + q^2 + ... + q^n = \frac{1 - q^{n+1}}{1 - q}$$

1. Exprimer la somme $1 + 6 + 6^2 + \cdots + 6^{n-1}$ à l'aide de cette propriété.
2. Montrer que pour tout entier naturel n, $6^n + 19$ est divisible par 5

2 Division euclidienne

► **Exercice 13**
Dans chacun des cas suivants, déterminer la division euclidienne de a par b.

$a = 247$ et $b = 6$

$a = 1111$ et $b = 11$

$a = 3874$ et $b = 50$

$a = 22$ et $b = 22745$

► **Exercice 14**
Si aujourd'hui nous sommes mercredi, quel jour serons-nous dans 100 jours ?

► **Exercice 15**
Sachant que $2253 \times 7 + 149 = 15920$, déterminer le quotient et le reste de la division euclidienne de 15920 par 7.

► **Exercice 16 — Numéro INSEE.**
Le numéro INSEE (ou numéro de sécurité sociale) est un numéro unique attribué à chaque individu en France. Il se compose de 15 chiffres

- le premier est 1 si l'individu est un homme et 2 si c'est une femme
- les deux chiffres suivants désignent les deux derniers chiffres de l'année de naissance
- les deux suivants correspondent au mois de naissance
- les deux suivants correspondent au département
- les trois suivants correspondent à la commune de naissance
- les trois suivants désignent le numéro d'inscription au registre de l'état civil
- les deux derniers sont une clé de contrôle qui permet de détecter les éventuelles erreurs de saisie

Cette clé de contrôle est calculé comme suit : On note A le nombre constitué des 13 premiers chiffres du numéro INSEE et R le reste de la division euclidienne de A par 97. La clé de contrôle vaut alors $C = 97 - R$. Si cette clé est entre 0 et 9, on ajoute des zéros en tête du nombre obtenu.

1. Justifier que la clé de contrôle est bien un numéro à deux chiffres
2. On considère un individu dont le numéro INSEE commence par 1 85 05 78 006 084
   (a) Déterminer le sexe, l'âge et le département de naissance de cet individu
   (b) Calculer la clé de contrôle de ce numéro INSEE.

► Exercice 17 — Chiffrement affine.
Le chiffrement est un procédé qui consiste à transformer un message clair en un message incompréhensible à toute personne n'ayant pas accès à la méthode de chiffrement. Une des méthodes de chiffrement possibles est le chiffrement affine. Les lettres de l'alphabet sont numérotées de 0 à 25.

On se donne alors deux entiers a et b et on considère la fonction $f : x \mapsto ax + b$. A chaque lettre x de l'alphabet, on associe alors le reste de la division euclidienne de $f(x)$ par 26. On remplace alors la lettre par la lettre correspondante.

Exemple : On considère la fonction $f : x \mapsto 7x + 2$. La lettre G porte le numéro 6. $f(2) = 7 \times 6 + 2 = 44$. Le reste de la division euclidienne de 44 par 26 est 18, qui correspond à la lettre S. On remplacera donc le G par la lettre S.

1. Compléter le tableau suivant, toujours en utilisant la fonction $f : x \mapsto 7x + 2$

Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$f(x)$							44						
Reste							18						
Lettre chiffrée							S						

Lettre en clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	13	14	15	16	17	18	19	20	21	22	23	24	25
$f(x)$													
Reste													
Lettre chiffrée													

2. A l'aide du tableau précédent, chiffrer le mot "MATHEMATIQUES"
3. A l'aide du tableau précédent, déchiffrer le mot "TGQFWGRE"
4. On considère désormais la fonction $f : x \mapsto 6x + 3$. Quelles seraient le résultat chiffré des lettres A et N ? Quel est le souci ?

► Exercice 18 — Avec des complexes.
Déterminer les valeurs de i^{2023} et $\left(\dfrac{\sqrt{2}}{2} + i\dfrac{\sqrt{2}}{2}\right)^{2023}$.

► Exercice 19
Soit n un entier naturel. Déterminer le reste de la division euclidienne de $5n + 11$ par $n + 2$.

► Exercice 20
Soit n un entier naturel. Déterminer, selon la valeur de n, le reste de la division euclidienne de $10n + 14$ par $4n + 3$.

▶ Exercice 21
Soit n un entier naturel

1. Déterminer la valeur des entiers relatifs a, b et c tels que
$$n^2+5=(an+b)(n+1)+c$$
2. En déduire les valeurs de n pour lesquelles n^2+5 est un multiple de $n+1$

▶ Exercice 22
Démontrer que le produit de deux nombres impairs est un nombre impair.

▶ Exercice 23
Soit n un entier naturel. Montrer que $(n+4)(n^2+7)$ est pair en raisonnant par disjonction de cas.

▶ Exercice 24
Soit n un entier naturel. Montrer que n^3-n est un multiple de 3 en raisonnant par disjonction de cas.

▶ Exercice 25
Soit n un entier naturel non multiple de 3.

1. Montrer que le reste de la division euclidienne de n^2 par 3 vaut 1
2. En déduire que n^2+9n+8 est divisible par 3.

▶ Exercice 26
Soit n un entier naturel. Montrer que $9n^3+36n^2-21n+30$ est un multiple de 6.

▶ Exercice 27
Soit n un entier naturel et $S_n=1^3+2^3+\cdots+n^3$

1. Montrer par récurrence que, pour tout entier naturel n,
$$S_n=\left(\frac{n(n+1)}{2}\right)^2$$
2. En déduire que S_n est un multiple de n si et seulement si n^3+2n^2+n est un multiple de 4.
3. En raisonnant par disjonction de cas, déterminer les entiers tels que S_n est un multiple de n.

3 Congruences

▶ Exercice 28
Dans chacun des cas suivants, compléter les pointillés en utilisant un nombre compris entre 0 et $n-1$, où n désigne le nombre entre crochets.

$17\equiv\ldots\ldots\,[5]$	$-14\equiv\ldots\ldots\,[3]$	$2214\equiv\ldots\ldots\,[2]$	$181\equiv\ldots\ldots\,[17]$
$-87\equiv\ldots\ldots\,[7]$	$999\equiv\ldots\ldots\,[11]$	$3165\equiv\ldots\ldots\,[3]$	$2500\equiv\ldots\ldots\,[11]$

▶ Exercice 29
Pour chacune des valeurs suivantes de a, trouver un entier relatif $b\in[\![-4;4]\!]$ tel que $a\equiv b\,[9]$

$a=18$ $a=47$ $a=897$ $a=111$ $a=2345$

► Exercice 30
Soit a un entier relatif tel que $a \equiv 68\,[26]$.

1. Quel est le reste de la division euclidienne de a par 26 ?
2. Quel est le reste de la division euclidienne de a par 13 ?

► Exercice 31
Déterminer l'ensemble des entiers relatifs n tels que $n \equiv 2\,[7]$ et $-20 \leqslant n \leqslant 30$.

► Exercice 32
Trouver un entier n tel que $n \equiv 3\,[7]$ et $n \equiv 2\,[9]$

► Exercice 33
Soit a un entier tel que $a \equiv 3\,[10]$. A-t-on également $a \equiv 3\,[5]$? La réciproque est-elle vraie ?

► Exercice 34
Soit n un entier naturel. On décompose n de la manière suivante :

$$n = a_0 + a_1 \times 10^1 + a_2 \times 10^2 + \cdots + a_p \times 10^p$$

où a_0, a_1, ..., a_p désignent des nombres entre 0 et 9. On admet qu'une telle décomposition est unique. Par exemple, $124 = 4 + 2 \times 10^1 + 1 \times 10^2$

1. Que vaut $n - a_0$? En déduire que tout entier est congrus à son dernier chiffre modulo 2, modulo 5 et modulo 10.
2. Montrer que tout entier naturel est congrus à l'entier formé par ses deux derniers chiffres modulo 25 et modulo 4.

4 Congruences et opérations

► Exercice 35
On considère l'entier $a = 1423 \times 26 + 149 \times 282$

1. A quoi sont congrus 1423, 26, 149 et 282 modulo 7 ?
2. En déduire que a est un multiple de 7.

► Exercice 36
Justifier que $5^2 \equiv -1[13]$ et en déduire que, pour tout entier naturel n, $5^{4n} - 1$ est un multiple de 13.

► Exercice 37
Montrer que, pour tout entier naturel a et b, on a $(a+b)^2 \equiv a^2 + b^2\,[2]$ et $(a+b)^3 \equiv a^3 + b^3\,[3]$.
A-t-on toujours $(a+b)^4 \equiv a^4 + b^4\,[4]$?

► Exercice 38
Soit n un entier relatif. En raisonnant par disjonction de cas selon les congruences de n modulo 6, montrer que $n(n+2)(7n-5)$ est un multiple de 6.

► Exercice 39
Exprimer en fonction de n le reste de la division euclidienne de 2^n par 5. En déduire le reste de la division euclidienne de 2022^{2022} par 5.

► Exercice 40
Soit n un entier naturel. On décompose n de la manière suivante :

$$n = a_0 + a_1 \times 10^1 + a_2 \times 10^2 + \cdots + a_p \times 10^p$$

où a_0, a_1, ..., a_p désignent des nombres entre 0 et 9. On admet qu'une telle décomposition est unique. Par exemple, $124 = 4 + 2 \times 10^1 + 1 \times 10^2$

1. Soit k un entier naturel. A quoi est congrus 10^k modulo 9 ?
2. En déduire que tout entier naturel est congrus à la somme de ses chiffres modulo 9.
3. Soit k un entier naturel. A quoi est congrus 10^k modulo 11 ?
4. Donner un critère de divisibilité par 11.

► Exercice 41 — Bac S, Novembre 2006.
Soit a un entier relatif. On appelle ordre de a modulo 7 le plus petit entier naturel k tel que $a^k \equiv 1\,[7]$.

1. Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1\,[6]$.
2. En déduire que k divise 6. Quelles sont les valeurs possibles de k ?
3. Donner l'ordre modulo 7 de tous les entiers compris entre 2 et 6 inclus.
4. Montrer que $2^{2006} + 3^{2006} + 4^{2006} + 5^{2006} + 6^{2006} \equiv 6\,[7]$.

► Exercice 42
Montrer que $2714^{1421} + 3419^{1324}$ est un multiple de 7.

► Exercice 43
Déterminer le chiffre des unités de 3^{2023}.

► Exercice 44 — Polynésie 2005.
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. Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n ?
2. Montrer que, pour tout entier naturel n, $u_{n+2} \equiv u_n\,[4]$.
3. En déduire que pour tout entier naturel k, $u_{2k} \equiv 2\,[4]$ et $u_{2k+1} \equiv 0\,[4]$.
4. (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, $2u_n \equiv 28\,[100]$.
5. Déterminer les deux derniers chiffres de l'écriture décimale de un suivant les valeurs de n.

► Exercice 45 — Montpellier - 1981.
Soit n un entier naturel

1. Trouver, suivant les valeurs de n, les restes de la division euclidienne de 5^n par 13.
2. En déduire que $1981^{1981} - 5$ est un multiple de 13.
3. Démontrer que, pour tout entier naturel n supérieur ou égal à 1, le nombre $N = 31^{4n+1} + 18^{4n-1}$ est divisible par 13.

► Exercice 46
Montrer que la somme de trois cubes consécutifs est divisibles par 9.

► Exercice 47
Montrer que pour tout entier naturel n, $3^{2n+1} + 2^{4n+2}$ est divisible par 7.