

Ouverture

Dans ce chapitre, la première partie du cours reprend les notions de divisibilité et de division euclidienne des entiers naturels, que les élèves connaissent depuis l'école primaire, pour les étendre aux entiers relatifs en donnant des définitions précises et en démontrant les propriétés qui en découlent.

Les entiers et leurs propriétés de divisibilité sont déjà étudiés dans le livre VII des *Éléments* d'**Euclide** (III^e siècle avant notre ère). On peut noter que la technique de la division euclidienne n'apparaît pas explicitement dans les *Éléments* ; l'algorithme que nous connaissons sous ce nom se rapproche cependant de l'algorithme des différences, exposé dans l'ouvrage. On ne peut pas dater avec précision son apparition, mais cette technique est présente de manière certaine à partir du XV^e siècle, dans les écrits d'**Al Kashi** vers 1430 et dans l'*Arithmétique* de Trévis (1478).

Une deuxième partie introduit une notion nouvelle pour les élèves de terminale S : celle d'arithmétique modulaire. Le principe d'égalité de deux entiers est remplacé par celui de congruence. Deux entiers sont congrus modulo n lorsqu'ils ont le même reste dans la division euclidienne par n . Ainsi sur l'horloge « 24 heures », l'heure indiquée sera identique 24 heures plus tard et il en sera de même toutes les 24 heures.

Les congruences ont été formalisées par **Carl Friedrich Gauss** dans *Disquisitiones Arithmeticae*, en 1801, généralisant une idée d'**Adrien-Marie Legendre** (1752-1833).

De nombreuses applications utilisent la notion de congruence : la démonstration des critères de divisibilité, les codes correcteurs d'erreurs tels que le dernier chiffre d'un numéro ISBN, la clé d'un numéro INSEE, la clé d'un numéro de carte bancaire...

Afin de motiver les élèves et suivant les consignes du programme, le choix a été fait d'aborder certaines de ces applications dans les activités préparatoires afin de montrer le rôle essentiel de la notion de restes égaux.

Questions d'approfondissement :

Il est 17 heures 15 minutes sur l'horloge.

- Quelle heure sera-t-il dans 2012^{2015} heures ?
- Quelle heure sera-t-il dans 2012^{2015} minutes ?

Réponse aux questions

a. On souhaite trouver le reste de la division euclidienne de 2012^{2015} par 24 et pour cela on raisonne « modulo 24 » :

$2\ 012 \equiv 20 \pmod{24}$, d'où $2\ 012^n \equiv 20^n \pmod{24}$. On étudie les restes modulo 24 des puissances successives de 20^n :

$$20^0 \equiv 1 \pmod{24}; 20^1 \equiv 20 \pmod{24}; 20^2 \equiv 16 \pmod{24};$$

$$20^3 \equiv 8 \pmod{24}; 20^4 \equiv 16 \pmod{24}.$$

On conjecture que la suite des restes est périodique de période 2 à partir de $n = 2$.

On montre par récurrence que pour tout entier k non nul, $20^{2k} \equiv 16 \pmod{24}$. On en déduit que pour tout entier k non nul, $20^{2k+1} \equiv 8 \pmod{24}$. Le reste modulo 24 de 20^n , donc de 2012^n , dépend par conséquent de la parité de n .

Pour tout entier naturel n supérieur ou égal à 2 : si n est pair, alors $20^n \equiv 16 \pmod{24}$; si n est impair, alors $20^n \equiv 8 \pmod{24}$. Comme $2\ 015$ est impair, $2\ 012^{2015} \equiv 8 \pmod{24}$. Le reste recherché est 8.

Or $17\ h\ 15 + 8\ h = 25\ h\ 15$. Il sera donc 01 h 15.

b. 1 jour = 24 heures = 1 440 minutes.

On souhaite trouver le reste de la division euclidienne de $2\ 012^{2015}$ par 1 440 et pour cela « on raisonne modulo 1 440 ». Ainsi $2\ 012 \equiv 572 \pmod{1440}$, d'où $2\ 012^n \equiv 572^n \pmod{1440}$.

On utilise un tableau pour examiner les restes modulo 1 440 des puissances successives de 572 :

n	Reste de 572^n	Reste de $1\ 216 \times 572^n$
0	1	1 216
1	572	32
2	304	1 024
3	1 088	1 088
4	256	256
5	992	992
6	64	64
7	608	608
8	736	736
9	512	512
10	544	544
11	128	128

n	Reste de 572^n	Reste de $1\,216 \times 572^n$
12	1 216	1216
13	32	32
14	1 024	1 024
15	1 088	1 088

On conjecture que la suite des restes est périodique de période 12 à partir de $n = 3$. Ceci nous conduit à étudier les restes modulo 1440 des entiers de la forme 572^{12k+p} .

On montre d'abord par récurrence que pour tout entier naturel k non nul : $572^{12k} \equiv 1216 [1440]$.

On en déduit que pour tout entier naturel k non nul et pour tout entier p compris entre 0 et 11 : $572^{12k+p} = 572^{12k} 572^p$ et

$$572^{12k+p} \equiv 1216 \times 572^p [1440].$$

En utilisant la 3^e colonne du tableau, on obtient donc :

$$572^{12k} \equiv 1216 [1440] ; 572^{12k+1} \equiv 32 [1440] \text{ et}$$

$$572^{12k+2} \equiv 1024 [1440]. \text{ Ainsi, pour tout entier } p \text{ compris entre 3 et 11 : } 572^{12k+p} \equiv 572^p [1440].$$

Ainsi le reste modulo 1 440 de 572^n , donc de $2\,012^n$, dépend du reste modulo 12 de n .

$$\text{On a } 2\,015 \equiv 11 [12], \text{ donc } 2\,012^{2015} \equiv 128 [1440].$$

Le reste cherché est donc 128.

Or 128 minutes = 2 heures 8 minutes.

17 h 15 + 2 h 08 = 19 h 23. Il sera donc 19 h 23.

Vérifier ses acquis

1 1. $a \in \mathbb{Q} ; b \in \mathbb{N} ; c \in \mathbb{Q} ; d \in \mathbb{R} ; e \in \mathbb{R} ; f \in \mathbb{Z}$.

2 a. Faux ; b. Vrai ; c. Vrai ; d. Faux.

2 a. Oui ($13^4 - 3^4 = (13 - 3)(13 + 3)(13^2 + 3^2)$).

b. Non (2 divise 436 et ne divise pas 56 879).

c. 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

3 a. Vrai ; b. Vrai ; c. Faux.

4 a. Vrai : $n = 6k \Rightarrow n = 3(2k)$.

b. Faux : 15 est divisible par 3 mais pas par 6.

c. Vrai : 5 et 6 sont premiers entre eux.

(Il n'est pas évident qu'un élève de TS sache justifier cette réponse en début d'année.)

d. Faux : 12 est divisible par 6 et 4 mais pas par 24.

e. Vrai : $a = 3k$ et $b = 3k' \Rightarrow a + b = 3(k + k')$.

5 $371 = 31 \times 11 + 30$ et $0 \leq 30 < 31$.

Le dividende est 371, le diviseur 31, le quotient 11 et le reste 30.

6 a. $45 = 2 \times 22 + 1$ et $0 \leq 1 < 2$;

b. $47 = 3 \times 15 + 2$ et $0 \leq 2 < 3$;

c. $497 = 23 \times 21 + 14$ et $0 \leq 14 < 23$;

d. $756 = 97 \times 7 + 77$ et $0 \leq 77 < 97$;

e. $750 = 27 \times 27 + 21$ et $0 \leq 21 < 27$.

7 $a = \frac{43}{57} ; b = \frac{71}{44} ; c = \frac{29}{14}$.

8 a. $\frac{35}{23} = 1 + \frac{12}{23} ;$ b. $-\frac{35}{23} = -2 + \frac{11}{23} ;$

c. $\frac{42}{13} = 3 + \frac{3}{13} ;$ d. $\frac{77}{4} = 19 + \frac{1}{4}$.

9 a. $n = 2k \Rightarrow n^2 = (2k)^2 = 2(2k^2)$

Donc, si n est pair, alors n^2 est pair.

b. $n = 2k + 1 \Rightarrow n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$.

Donc, si n est impair, alors n^2 est impair.

c. Soit un entier naturel n tel que n^2 est pair.

On raisonne par l'absurde : si n était impair d'après b., n^2 serait impair, ce qui est contraire à l'hypothèse. Donc n est pair.

d. Soit n un entier naturel tel que n^2 est impair.

On raisonne, de même, par l'absurde : si n était pair alors n^2 serait pair d'après a., ce qui est contraire à l'hypothèse. Donc n est impair.

e. On envisage les deux cas :

• n est pair et s'écrit $n = 2k$ et alors

$$n(n + 1) = 2k(2k + 1) \text{ est pair ;}$$

• n est impair et s'écrit $n = 2k + 1$ et alors

$$n(n + 1) = (2k + 1)(2k + 2) = 2(2k + 1)(k + 1) \text{ est pair.}$$

10 a. $32 + 23 = 55 ; 94 + 49 = 143$ et $57 + 75 = 132$ sont des multiples de 11.

b. Soit $n = \overline{ab}$ et $n' = \overline{ba}$ dans le système décimal. On a $n + n' = 10a + b + 10b + a = 11(a + b)$, donc $n + n'$ est un multiple de 11.

11 a. Soit $n = \overline{aaa}$ dans le système décimal.

$$n = 100a + 10a + a = 111a = 37 \times 3 \times a, \text{ donc } n \text{ est un multiple de } 37.$$

b. Soit $n' = \overline{aaaaaa}$ dans le système décimal.

$$n' = 1\,000n + n = 1\,001n. \text{ Or d'après a. } n \text{ est un multiple de } 37, \text{ donc } n' \text{ est aussi un multiple de } 37.$$

Activités d'introduction

Activité 1

1 a. La courbe $\mathcal{C}_1$ d'équation $2x + 4y = 5$ est une droite.

b. Elle ne semble pas contenir de point à coordonnées entières.

c. S'il existait un point à coordonnées entières, 2 devrait diviser $2(x + 2y)$ et donc devrait diviser 5, ce qui est faux. Il n'existe donc pas de point à coordonnées entières sur cette droite.

2 a. La courbe $\mathcal{C}_2$ d'équation $xy = 10$ ou $y = \frac{10}{x}$ est une hyperbole.

b. Il semble que la branche de $\mathcal{C}_2$ située dans le quart de plan ($x > 0$ et $y > 0$) contient quatre points à coordonnées entières.

c. On constate que x et y sont deux diviseurs positifs associés de 10, c'est-à-dire $(x; y) = (1; 10)$ ou $(x; y) = (10; 1)$ ou $(x; y) = (2; 5)$ ou $(x; y) = (5; 2)$.

d. La courbe étant symétrique par rapport à l'origine, on en déduit quatre autres points à coordonnées entières situés sur l'autre branche de la courbe : $(-1; -10)$; $(-10; -1)$; $(-2; -5)$ et $(-5; -2)$.

3 $x^2 - y^2 = 7 \Leftrightarrow (x - y)(x + y) = 7$.

S'il existe $(x; y)$, couple d'entiers naturels tel que $x^2 - y^2 = 7$ alors $x - y$ et $x + y$ sont deux diviseurs positifs associés de 7 tels que $x - y < x + y$. D'où :

$$\begin{cases} x - y = 1 \\ x + y = 7 \end{cases} \Leftrightarrow \begin{cases} x = 4 \\ y = 3 \end{cases}. \text{ On vérifie que ce couple}$$

convient et par symétrie de la courbe par rapport à l'origine et l'axe des ordonnées, on déduit trois autres points : $(-4; -3)$; $(-4; 3)$; $(4; -3)$.

4 a. $\mathcal{C}_4$ est le cercle de centre l'origine et de rayon $\sqrt{7}$.

b. La courbe $\mathcal{C}_4$ ne semble pas contenir de point à coordonnées entières.

c. $x^2 + y^2 = 7$, d'où $0 \leq x^2 \leq 7$ et $0 \leq y^2 \leq 7$.

On remarque que x et y étant entiers, on a : $0 < x^2 < 7$ et $0 < y^2 < 7$. Or les seuls entiers dont les carrés vérifient ces conditions sont : $-1, 1, -2$ et 2 . Puisque $1 + 1 \neq 7$ et $1 + 4 \neq 7$ et $4 + 4 \neq 7$, il n'existe pas de couple d'entiers tel que $x^2 + y^2 = 7$. Donc $\mathcal{C}_4$ ne contient aucun point à coordonnées entières.

Activité 2

1 a. Le 29 janvier 2011 était un samedi.

Dans un tableur, on utilise la formule :

" = JOURSEM(DATE(2011 ; 1 ; 29) ; 1)" =

b. 28 jours se sont écoulés entre le 1^{er} janvier 2011 et le 29 janvier 2011.

Dans un tableur, on utilise la formule :

" = DATE(2011 ; 1 ; 29) - DATE(2011 ; 1 ; 1)" =

c. Entre le 1^{er} janvier 2011 et chaque samedi du mois, il s'est écoulé 7 jours, puis 14 jours, puis 21, puis 28 jours. On remarque que 7, 14, 21 et 28 sont des multiples de 7.

d. Les nombres de jours écoulés entre le 1^{er} janvier 2011 et chaque dimanche du mois sont : 1, 8, 15, 22, 29, entiers naturels de la forme $1 + 7k$. De même, les nombres de jours écoulés entre le 1^{er} janvier et chaque lundi sont : 2, 9, 16, 23, 30, entiers de la forme $2 + 7k$; entre le 1^{er} janvier et chaque mardi il s'est écoulé : 3, 10, 17, 24, 31 jours (entiers de la forme $3 + 7k$); et entre le 1^{er} janvier et chaque mercredi il s'est écoulé : 4, 11, 18, 25 jours (entiers de la forme $4 + 7k$)...

En conclusion, tout semble dépendre du reste de la division euclidienne par 7 du nombre de jours écoulés.

2 a. Entre le 1^{er} janvier 2011 et le 21 mars 2011, il s'est écoulé $31 + 28 + 20 = 79$ jours.

b. et c. $79 = 7 \times 11 + 2$ et $0 \leq 2 < 7$. Ici $q = 11$ et $r = 2$.

d. Il s'est écoulé 11 semaines pleines et 2 jours, donc le 21 mars 2011 était un lundi.

3 $N = 6 \times 31 + 4 \times 30 + 28 + 24 = 358$.

Or $358 = 7 \times 51 + 1$ et $0 \leq 1 < 7$. Donc le 25 décembre 2011 était un dimanche.

4 $N = 365 + 366 + 358 = 1\,089$.

Or $1\,089 = 7 \times 155 + 4$ et $0 \leq 4 < 7$. Donc le 25 décembre 2013 est un mercredi.

Activité 3

Objectif : Introduire des propriétés de $\mathbb{N}$ puis définir la partie entière d'un réel.

1 a. 0 est le plus petit élément de $\mathbb{N}$.

$\mathbb{N}$ n'a pas de plus grand élément : quel que soit l'entier naturel n , il existe un entier naturel $n' = n + 1$ tel que $n' > n$.

b. $A = \{0; 1; 2; 3\}$, on en déduit que A est non vide, qu'il a un plus grand élément 3, et qu'il est majoré par exemple par 3.

c. $I =]2; 15[$ n'a ni de plus petit élément ni de plus grand élément.

d. En revanche

$J = I \cap \mathbb{N} = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ a un plus petit élément 3 et un plus grand élément 14.

Le but de ces questions est d'introduire les propriétés fondamentales suivantes de $\mathbb{N}$:

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Toute partie non vide de $\mathbb{N}$ et majorée admet un plus grand élément.

2 Il semble que pour tout réel x , il existe un seul entier n tel que $n \leq x < n+1$.

3 a. $M = \{n \in \mathbb{N} | n \leq x\}$ est une partie non vide de $\mathbb{N}$ (elle contient 0), elle est majorée par x , on en déduit qu'elle contient un plus grand élément noté q .

b. $q \in M$, donc $q \leq x$ mais $q+1 \notin \mathbb{N}$ et $q+1 \notin M$, donc $x < q+1$. Donc, $q \leq x < q+1$.

c. Soient deux entiers q et q' tels que $q \leq x < q+1$ et $q' \leq x < q'+1$, on en déduit :

$-1 < q - q' < 1$, d'où $q - q' = 0$, soit $q = q'$. Donc pour tout réel positif ou nul x il existe un seul entier naturel q tel que $q \leq x < q+1$.

4 Soit x un nombre négatif. S'il est entier relatif, le résultat est évident. Sinon, en considérant $-x$, nombre positif non entier, d'après la première partie, il existe un unique entier q tel que $q < -x < q+1$. Il en résulte $-q-1 < x < -q$ et en posant $q' = -q-1$ on déduit $q' \leq x < q'+1$. On montre comme pour le cas « $x > 0$ » l'unicité de q' .

5 a. $E(-3) = -3$; $E(-3,5) = -4$; $E(-2,3) = -3$; $E(-0,5) = -1$; $E(0,5) = 0$; $E(1,5) = 1$.

b. Attention sur TI : $\text{PartEnt} \neq \text{Ent}$ et sur Casio : $\text{Intg} \neq \text{Int}$

6 a. Les entiers naturels q et r sont le quotient et le reste de la division euclidienne de l'entier naturel a par l'entier naturel non nul b si et seulement si $a = bq + r$ et $0 \leq r < b$.

b. On en déduit : $0 \leq a - bq < b$, soit $bq \leq a < b(q+1)$, soit, puisque $b > 0$:

$q \leq \frac{a}{b} < q+1$; q est donc la partie entière de $\frac{a}{b}$.

c.

Lire a et b (b non nul)

Afficher « q = » ; E(a/b)

Afficher « r = » ; a-bE(a/b)

d. $q = 8$ et $r = 3$.

Activité 4

1 a. $3(7+2+0+1+8+3) + (9+8+7+1+5+3+4) = 100$.

b. Pour C_1 , $3(7+2+0+1+7+3) + (9+8+7+1+5+3+4) = 97$.

Pour C_2 , $3(7+2+0+1+8+3) + (9+8+7+7+5+3+4) = 106$.

Dans les deux cas les codes ne sont pas corrects.

c. $3(7+2+0+1+3+3) + (9+8+7+1+5+8+4) = 90$.

Il semble que l'erreur n'ait pas été détectée, c'est normal car $3(8-3) + 3-8 = 20$ est un multiple de 10.

2 a. $3(2+1+4+0+1+6) + (3+5+2+1+4+7+x) = 42+22+x = 64+x$. x est un entier tel que $0 \leq x \leq 9$ et $64+x$ est un multiple de 10, donc $x = 6$.

b. Il suffit de modifier les chiffres afin d'ajouter à cette somme un multiple de 10.

Par exemple $C_5 = 3\ 251261\ 041746$,

$C_6 = 3\ 251741\ 041266$ et

$C_7 = 3\ 251216\ 041746$ ont la même clé que

$C_4 = 3\ 251241\ 041766$.

c. $N = 10d + u$ avec $0 \leq u \leq 9$. a_{13} vérifie la condition $N + a_{13} = 10d + u + a_{13}$ est un multiple de 10, d'où $a_{13} = 10 - u$.

3 a. Un seul chiffre est erroné : a_k est remplacé par b_k . On distingue deux cas :

• Si k est impair, cela revient à ajouter $d = b_k - a_k$

à $N' = 3 \times \left(\sum_{i=1}^6 a_{2i} \right) + \sum_{i=0}^6 a_{2i+1}$. L'erreur n'est pas

détectée si et seulement si cette différence est un multiple de 10.

Or $0 \leq a_k \leq 9$ et $0 \leq b_k \leq 9$ impliquent que

$-9 \leq b_k - a_k \leq 9$, et le seul multiple de 10 compris entre -9 et 9 est 0, ce qui correspond à $a_k = b_k$. Donc une telle erreur est toujours détectée.

• Si k est pair, cela revient à ajouter $d = 3(b_k - a_k)$ à N' . Or $-9 \leq b_k - a_k \leq 9 \Rightarrow -27 \leq 3(b_k - a_k) \leq 27$ et le seul multiple de 10 et 3 compris entre -27 et 27 est 0, d'où $a_k = b_k$. Donc une telle erreur est toujours détectée.

b. Intervertir deux chiffres consécutifs revient par exemple à remplacer dans N' , $3a_k + a_{k+1}$ par $a_k + 3a_{k+1}$, ce qui revient à ajouter $d = a_k + 3a_{k+1} - (3a_k + a_{k+1}) = 2(a_{k+1} - a_k)$. On en déduit que l'erreur n'est pas détectée si seulement si $a_{k+1} - a_k = 5$ ou -5 .

4 $3(2+2+3+0+1+6) + (3+5+x+7+4+7+7) = 75+x$, d'où $x = 5$.

Activité 5

1 $r = N - (E(N/97)) = 12$, d'où
 $K = 97 - r = 97 - 12 = 85$.

2 a. $N = 2\,840\,492 \times 10^6 + 019\,081$, d'où
 $A = 2\,840\,492$ et $B = 019\,081$.

b. $10^6 = 97 \times 10309 + 27$.

$A = 97 \times 29283 + 41$ d'où $r_1 = 41$;

$B = 97 \times 196 + 69$ d'où $r_2 = 69$.

c. $N' = 27r_1 + r_2 = 27 \times 41 + 69 = 1\,176$.

$1\,176 = 97 \times 12 + 12$, on retrouve le reste $r = 12$ de la question 1.

d. $a = 97q_1 + r_1$ et $0 \leq r_1 < 97$;

$b = 97q_2 + r_2$ et $0 \leq r_2 < 97$.

On en déduit que :

$a + b = 97(q_1 + q_2) + r_1 + r_2$ et donc si

$r_1 + r_2 = 97Q + R$ avec $0 \leq R < 97$ alors :

$a + b = 97(q_1 + q_2 + Q) + R$ et $0 \leq R < 97$; donc

dans la division euclidienne par 97, $a + b$ et $r_1 + r_2$ ont le même reste.

$ab = 97(97q_1q_2 + r_1q_2 + r_2q_1) + r_1r_2$ et si

$r_1r_2 = 97Q' + R'$ avec $0 \leq R' < 97$, alors :

$ab = 97(97q_1q_2 + r_1q_2 + r_2q_1 + Q') + R'$ et

$0 \leq R' < 97$; donc ab et r_1r_2 ont le même reste.

Par suite, 10^6a a le même reste que $27r_1$ et

$N = 10^6a + b$ a le même reste que $27r_1 + r_2$.

3 a. Soit $N_1 = 2\,84\,04\,22\,019\,081$.

$A = 2\,840\,422$ et $B = 019\,081$;

$r_1 = 68$ et $r_2 = 69$.

$N' = 27 \times 68 + 69 = 1\,905 = 97 \times 19 + 62$ d'où

$r = 62$ et $K = 97 - 62 = 35$.

b. Soit $N_2 = 2\,48\,04\,92\,019\,081$.

$A = 2\,480\,492$ et $B = 019\,081$;

$r_1 = 8$ et $r_2 = 69$.

$N' = 27 \times 8 + 69 = 285 = 97 \times 2 + 91$ d'où $r = 91$ et $K = 97 - 91 = 06$.

c. Il semble que si un seul chiffre est faux l'erreur est décelable car cela revient à ajouter à N , $a \times 10^n$ avec $0 < a < 10$, ce qui modifie le reste puisque $a \times 10^n$ n'est pas divisible par 97.

De même, si on intervertit deux chiffres consécutifs distincts, cela revient à ajouter un entier du type $a10^n + b10^{n+1} - b10^n - a10^{n+1} =$

$10^n(a + 10b - b - 10a) = 10^n(9b - 9a) = 9 \times 10^n(b - a)$

où $b - a$ est un entier non nul compris entre -9 et 9 . Ce nombre n'étant pas divisible par 97 (ce qui sera démontré rigoureusement dans les chapitres suivants), le reste est donc modifié et l'erreur est ainsi décelée.

d. Si une erreur revient à ajouter un multiple de 97, cette erreur ne sera pas décelée.

Par exemple $N + 97$ a la même clé que N .

Activité 6

1 a. E : $n = 4$; $3n + 5 = 17$; $r = 17$; code = R
 U : $n = 20$; $3n + 5 = 65$; $r = 13$; code = N
 C : $n = 2$; $3n + 5 = 11$; $r = 11$; code = L
 L : $n = 11$; $3n + 5 = 38$; $r = 12$; code = M
 I : $n = 8$; $3n + 5 = 29$; $r = 3$; code = D
 D : $n = 3$; $3n + 5 = 14$; $r = 14$; code = O
 E : $n = 4$; $3n + 5 = 17$; $r = 17$; code = R
 EUCLIDE est codé par RNLMODOR.

b.

lettre	A	B	C	D	E	F	G	H	I
n	0	1	2	3	4	5	6	7	8
n'	5	8	11	14	17	20	23	0	3
code	F	I	L	O	R	U	X	A	D
lettre	J	K	L	M	N	O	P	Q	R
n	9	10	11	12	13	14	15	16	17
n'	6	9	12	15	18	21	24	1	4
code	G	J	M	P	S	V	Y	B	E
lettre	S	T	U	V	W	X	Y	Z	
n	18	19	20	21	22	23	24	25	
n'	7	10	13	16	19	22	25	2	
code	H	K	N	Q	T	W	Z	C	

Pour le remplir

1	A	Voir explication TP TICE 3 page 24
2	= CODE(A1)–65	
3	= MOD(3*A2 + 5 ; 26)	
4	= CAR(A3 + 65)	

D'après le tableau ci-dessus, le nom codé par XFNHH est GAUSS.

2 a.

R : $n = 17$; $13n + 4 = 225$; $n' = 17$; code = R

A : $n = 0$; $13n + 4 = 4$; $n' = 4$; code = E

G : $n = 6$; $13n + 4 = 82$; $n' = 4$; code = E

E : $n = 4$; $13n + 4 = 56$; $n' = 4$; code = E

Donc RAGE est codé par REEE.

P : $n = 15$; $13n + 4 = 199$; $n' = 17$; code = R

E : _____ code = E

A : _____ code = E

U : $n = 20$; $13n + 4 = 264$; $n' = 4$; code = E.

Donc PEAU est aussi codé par REEE

b. On remarque que deux mots distincts sont codés de la même façon.

c. Ce chiffrement code des lettres distinctes par une même lettre et n'est donc pas considéré comme un bon chiffrement.

3 On trouvera des réponses dans le chapitre suivant. Remarque : les « bonnes clés » sont, dans cette activité, les clés codant deux lettres distinctes par deux lettres distinctes.

Travaux pratiques

TP Algorithmique 1 Deux algorithmes

Le premier algorithme affiche tous les diviseurs de A.

Le second affiche le quotient et le reste de la division euclidienne de A par B.

Amélioration : pour le premier on peut utiliser les diviseurs associés, en faisant attention lorsque A est un carré d'entier car la condition devient $l \leq \sqrt{A}$.

```

Lire A (entier non nul)
Pour l allant de 1 à  $\sqrt{A}$  faire
    Si partie fractionnaire de  $\frac{A}{l}$  est 0 alors
        Afficher l
        Si  $A \neq l^2$  alors
            Afficher  $\frac{A}{l}$ 
        FinSi
    FinSi
FinPour
  
```

Pour le second on peut utiliser les fonctions QUOTIENT et MOD.

TP Algorithmique 2 Problèmes de numération

b est un entier naturel supérieur ou égal à 2 et a est un entier naturel non nul.

1 a. i. Comme $\lim b^n = +\infty$, alors pour tout réel A, il existe N tel que si $n \geq N$ alors $b^n > A$. En particulier il existe k_0 tel que $b^{k_0} > a$.

ii. $M = \{k \in \mathbb{N} | b^k > a\}$ est une partie de $\mathbb{N}$ non vide (elle contient k_0), elle admet donc un plus petit élément qui peut s'écrire $n + 1$:

$n + 1 \in M$, d'où $a < b^{n+1}$, mais $n \notin M$, d'où $b^n \leq a$. Donc $b^n \leq a < b^{n+1}$.

iii. Dans cette question on veut montrer que $0 < a_n < b$.

Par division euclidienne de a par b^n : il existe deux entiers naturels a_n et r_n tels que $a = a_n b^n + r_n$ avec $0 \leq r_n < b^n$.

$a \geq b^n$, d'où $a_n > 0$ et $a_n b^n \leq a < b^{n+1}$, d'où $a_n < b$. Donc : $0 < a_n < b$.

iv. Si $n = 0$, on a alors $a = a \times 10^0 + 0$, d'où $a_0 = a$ et $r_0 = 0$.

Si $n > 0$, alors par division euclidienne de r_n par b^{n-1} :

$r_n = a_{n-1} b^{n-1} + r_{n-1}$ avec $0 \leq r_{n-1} < b^{n-1}$, d'où $0 \leq a_{n-1} < b$ (a_{n-1} peut être nul, ce qui n'est pas le cas pour a_n).

Si $n > 1$, on recommence avec r_{n-1} et on construit une suite finie d'entiers $(a_n, a_{n-1}, \dots, a_i, \dots, a_0)$ avec :

$0 < a_n < b$ et pour $0 \leq i < n$, $0 \leq a_i < b$ et $r_{i+1} = a_i b^i + r_i$ et $0 \leq r_i < b^i$ (en particulier $r_0 = 0$).

On obtient alors :

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

b. Soit $a = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b^1 + a_0$ tel que pour tout i , $a_i \in \mathbb{N}$ et $0 \leq a_i < b$ et $a_n \neq 0$.

i. $a = b(a_n b^{n-1} + a_{n-1} b^{n-2} + \dots + a_1) + a_0$ et $0 \leq a_0 < b$, donc a_0 est le reste de la division de a par b.

ii. Le quotient est

$q_0 = a_n b^{n-1} + a_{n-1} b^{n-2} + \dots + a_1$ et $q_0 < a$.

iii. $q_0 = b(a_n b^{n-2} + a_{n-1} b^{n-3} + \dots + a_2) + a_1$ et $0 \leq a_1 < b$.

a_1 est donc le reste de la division de q_0 par b.

Le quotient est $q_1 = a_n b^{n-2} + a_{n-1} b^{n-3} + \dots + a_2$ et $q_1 < q_0 < a$.

iv. Ainsi on construit une suite strictement décroissante $a_n = q_{n-1} < q_{n-2} < \dots < q_1 < q_0 < a$ telle que, pour i allant de 1 à $n - 1$, a_i est le reste de la division de q_{i-1} par b et $a_n = q_{n-1}$.

c. i. a_0 est le reste de la division euclidienne de a par b : $a = b q_0 + a_0$ et $0 \leq a_0 < b$.

a_1 est le reste de la division de q_0 par b :

$q_0 = b q_1 + a_1$ et $0 \leq a_1 < b$.

Pour i de 1 à $n - 1$, a_i est le reste de la division euclidienne de q_{i-1} par b et q_i le quotient.

a_{n-1} est le reste de la division de q_{n-2} par b et a_n est le quotient de cette division, c'est-à-dire q_{n-1} .

Puisque $0 \leq a_i < b$, on en déduit que les a_i prennent les valeurs : 0, 1, 2, 3, ..., $b - 1$, cela donne b « chiffres ».

ii. Algorithme de changement de base de la base 10 à la base B :

Lire N, B

A = 0 et E = 0

Tant Que N ≠ 0 faire

$$R = N - \text{Ent} \left(\frac{N}{B} \right) * B$$

$$A = A + R * 10^E$$

$$E = E + 1$$

$$N = \frac{N - R}{B}$$

FinTantque

Afficher A

iii. On trouve $7^8 = 5\,764\,801$.

2. a. i. $1\,341 = 10^3 + 3 \times 10^2 + 4 \times 10 + 1$.

ii. $10^3 < N < 10^4$.

b. i. En base deux, deux chiffres sont utilisés (0 et 1).

ii. $A = 111...1\,111 = 1 + 2 + 2^2 + \dots + 2^{n-1} = \frac{1-2^n}{1-2} = 2^n - 1$.

c. i.

+	0	1
0	0	1
1	1	0

Ainsi $A + B = 11\,000$

×	0	1
0	0	0
1	0	1

Ainsi $A \times B = 10\,001\,111$

ii. Vérification en base dix : $A = 1 + 2^2 + 2^3 = 13$;
 $B = 1 + 2 + 2^3 = 11$.

$A + B = 2^3 + 2^4 = 24$ et $11 + 13 = 24$.

$A \times B = 1 + 2 + 2^2 + 2^3 + 2^7 = 143$ et

$11 \times 13 = 143$.

TP TICE 1 Critères de divisibilité

Objectif : utiliser les congruences pour démontrer les critères de divisibilité.

1 a. $10 - 1 = 9$, donc 9 divise $10 - 1$, donc $10 \equiv 1[9]$.

On en déduit, pour tout entier naturel n , $10^n \equiv 1^n[9]$ soit $10^n \equiv 1[9]$

b. On en déduit, pour tout entier naturel k compris entre 1 et n : $a_k 10^k \equiv a_k[9]$, et en sommant ces congruences :

$$a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10^1 + a_0$$

$$\equiv a_n + a_{n-1} + \dots + a_1 + a_0[9]$$

soit $a \equiv a_n + a_{n-1} + \dots + a_1 + a_0[9]$

c. Or 9 divise a si et seulement si $a \equiv 0[9]$.

Puisque $a \equiv a_n + a_{n-1} + \dots + a_1 + a_0[9]$, 9 divise a si et seulement si 9 divise $a_n + a_{n-1} + \dots + a_1 + a_0$.

On a démontré le critère de divisibilité par 9 : un entier naturel est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

d. $10 - 3 \times 3 = 1$, d'où $10 \equiv 1[3]$, d'où pour tout entier naturel k , $10^k \equiv 1[3]$ et on raisonne ensuite comme dans **b.** et **c.** On obtient donc le critère de divisibilité par 3 : un entier naturel est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

Application :

$N = 201\,527\,120\,112\,011\,925$ est divisible par 3 car la somme de ses chiffres est égale à 42 qui est divisible par 3.

2 a.

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10^1 + a_0$$

$$= 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \dots + a_1) + a_0$$

$$= 10q + u, \text{ avec}$$

$$q = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \dots + a_2 10^1 + a_1$$

$$\text{et } u = a_0.$$

$$10 \equiv 0[2] \Rightarrow 10q \equiv 0[2] \Rightarrow 10q + u \equiv u[2];$$

$$10 \equiv 0[5] \Rightarrow 10q \equiv 0[5] \Rightarrow 10q + u \equiv u[5];$$

on en déduit que $a \equiv u[2]$ et $a \equiv u[5]$.

b. On en déduit les critères connus :

a est divisible par 2 (ou 5) si et seulement si son chiffre des unités u est divisible par 2 (ou 5).

3 a. $10 - (-1) = 11$, donc 11 divise $10 - (-1)$, donc $10 \equiv (-1)[11]$.

On en déduit, pour tout entier naturel k ,

$$10^k \equiv (-1)^k[11]$$

b. On en déduit, pour tout entier naturel k compris entre 1 et n : $a_k 10^k \equiv a_k (-1)^k[11]$, donc

si $k = 2p$ alors

$$a_{2p} 10^{2p} \equiv a_{2p} (-1)^{2p}[11] \text{ soit } a_{2p} 10^{2p} \equiv a_{2p}[11]$$

si $k = 2p + 1$ alors

$$a_{2p+1} 10^{2p+1} \equiv a_{2p+1} (-1)^{2p+1}[11]$$

$$\text{soit } a_{2p+1} 10^{2p+1} \equiv -a_{2p+1}[11].$$

En sommant ces congruences on obtient :

$$a_0 + a_1 10^1 + a_2 10^2 + a_3 10^3 + \dots + a_{n-1} 10^{n-1} + a_n 10^n$$

$$\equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^{n-1} a_{n-1} + (-1)^n a_n[11]$$

$$\text{soit } a \equiv (a_0 + a_2 + a_4 \dots) - (a_1 + a_3 + a_5 + \dots)[11].$$

c. On en déduit qu'un entier a est divisible par 11 si et seulement si la somme alternée des chiffres $a_0 - a_1 + a_2 - a_3 + \dots + (-1)^{n-1}a_{n-1} + (-1)^na_n$ est divisible par 11.

4 a.

N	0	1	2	3	4	5
$10^n \bmod 7$	1	3	2	-1	-3	-2
N	6	7	8	9	10	11
$10^n \bmod 7$	1	3	2	-1	-3	-2

b. On constate que les restes sont périodiques de période 6.

c. On a donc

$$10^0 \equiv 1[7]; 10^1 \equiv 3[7];$$

$$10^2 \equiv 3^2[7] \text{ soit } 10^2 \equiv 2[7];$$

$$10^3 \equiv 3 \times 2[7] \text{ soit } 10^3 \equiv -1[7];$$

$$10^4 \equiv -3[7]; 10^5 \equiv -2[7];$$

$$10^6 \equiv 3 \times (-2)[7] \text{ soit } 10^6 \equiv 1[7]$$

Puisque $10^6 \equiv 1[7]$, pour tout entier naturel q , $(10^6)^q \equiv 1^q[7]$ soit $10^{6q} \equiv 1[7]$ d'où pour r entier compris entre 0 et 5 : $10^{6q} \times 10^r \equiv 10^r[7]$, soit $10^{6q+r} \equiv 10^r[7]$.

Ainsi :

$$10^{6k} \equiv 1[7]; 10^{6k+1} \equiv 3[7]; 10^{6k+2} \equiv 2[7];$$

$$10^{6k+3} \equiv -1[7]; 10^{6k+4} \equiv -3[7]; 10^{6k+5} \equiv -2[7].$$

d. On en déduit que $a = a_8a_7a_6a_5a_4a_3a_2a_1a_0$ est congru modulo 7 au nombre

$$N = (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8)$$

et donc a est divisible par 7 si et seulement si N est divisible par 7.

Pour $a = 798\,342\,752$, $N = (2 + 3 \times 5 + 2 \times 7) - (2 + 3 \times 4 + 2 \times 3) + (8 + 3 \times 9 + 2 \times 7) = 60$ n'est pas divisible par 7, donc a n'est pas divisible par 7. Pour $a = 688\,243\,157$, $N = 49$ est divisible par 7, donc a est divisible par 7.

e. On peut énoncer un critère de divisibilité par 7 : $a = a_8a_7a_6a_5a_4a_3a_2a_1a_0$ est divisible par 7 si et seulement si $N = (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + \dots)$ est divisible par 7.

Exemple d'algorithme :

```

Lire N
A ← 0 : E ← 0
L1 ← {1, 3, 2}
TantQue Ent(  $\frac{N}{10^E}$  ) ≠ 0 faire
    Pour i allant de 1 à 3 faire
        A ← A + (-1)E * Ent(  $\left[ \text{pardéc} \left( \frac{N}{10^{E+i}} \right) * 10 \right]$  )
        * L1(i)
    FinPour
    E ← E + 3
FinTantQue
Si mod(A, 7) = 0 alors
    Afficher « N » est divisible par 7
Sinon
    Afficher « N » n'est pas divisible par 7
FinSi

```

5

$$10^0 \equiv 1[13]; 10^1 \equiv -3[13];$$

$$10^2 \equiv (-3)^2[13] \text{ soit } 10^2 \equiv -4[13];$$

$$10^3 \equiv (-3)(-4)[13] \text{ soit } 10^3 \equiv -1[13];$$

$$10^4 \equiv 3[13]; 10^5 \equiv 4[13];$$

$$10^6 \equiv (-3) \times 4[13] \text{ soit } 10^6 \equiv 1[13];$$

De plus, pour tous les entiers naturels q et r $10^{6q+r} \equiv 10^r[13]$.

On en déduit que $a = a_8a_7a_6a_5a_4a_3a_2a_1a_0$ est congru modulo 13 au nombre $N = (a_0 - 3a_1 - 4a_2) - (a_3 - 3a_4 - 4a_5) + (a_6 - 3a_7 - 4a_8)$ et donc a est divisible par 13 si et seulement si N est divisible par 13

TP TICE 2 Restes modulo p

1 et **2**

	a = 5				b = -3				p = 20			
n	0	1	2	3	4	5	6	7	8			
u_n	-3	2	7	12	17	22	27	32	37			
reste modulo p	17	2	7	12	17	2	7	12	17			
	a = 5				b = -3				p = 7			
n	0	1	2	3	4	5	6	7	8			
u_n	-3	2	7	12	17	22	27	32	37			
reste modulo p	4	2	0	5	3	1	6	4	2			

On conjecture que la suite des restes est périodique de période 4 dans le 1^{er} cas et de période 7 dans le 2nd cas.

3 a. Les nombres $u_0, u_1, \dots, u_p$ forment une famille de cardinal $p + 1$. Or il y a p restes différents possibles dans une division par p .

D'après le principe des tiroirs, il existe au moins deux entiers parmi $u_0, u_1, \dots, u_p$ qui ont le même reste dans la division euclidienne par p .

b. Par hypothèse u_{n_0} et u_{n_0+T} ont le même reste dans la division euclidienne par p , il en découle que $u_{n_0+T} - u_{n_0}$ est un multiple de p .

Or $u_{n_0+T} - u_{n_0} = (a(n_0 + T) + b) - (an_0 + b) = aT$.

Donc aT est un multiple de p .

c. On pose $aT = qp$ avec $q \in \mathbb{N}$.

Pour tout entier k de $\mathbb{N}$, on a :

$u_{T+k} = a(T + k) + b = (ak + b) + aT = u_k + qp$.

Ainsi la différence $u_{T+k} - u_k$ est divisible par p , cela signifie que u_{T+k} et u_k ont le même reste dans la division euclidienne par p .

La suite des restes est donc T -périodique.

TP TICE 3 Coder et décoder avec un chiffrement affine

1 a.

	A
2	= CODE(A1)–65
3	= MOD(17*A2 + 5 ; 26)
4	= CAR(A3 + 65)

Ce qui donne :

P	O	I	N	C	A	R	E
15	14	8	13	2	0	17	4
0	9	11	18	13	5	8	21
A	J	L	S	N	F	I	V

b. Message codé en majuscules :

NVZQAFIKFKJDLRHRVHVSJHZAIJHYJSZNVZQA
FIKLSQHLQLJSRHSVJHZLSYVSQJSZ

2 a. i. Entrer en B2 « = MOD(B\$1*\$A2 ; 26) ».

On peut se contenter de la table de multiplication par 17 modulo 26 :

x	0	1	2	3	4	5	6	7	8
17x	0	17	8	25	16	7	24	15	6
x	9	10	11	12	13	14	15	16	17
17x	23	14	5	22	13	4	21	12	3
x	18	19	20	21	22	23	24	25	
17x	20	11	2	19	10	1	18	9	

ii. Il existe un seul entier naturel compris entre 0 et 25 tel que $17u \equiv 1[26]$, c'est $u = 23$. On a donc : $23 \times 17 \equiv 1[26]$.

iii.

$y \equiv 17x + 5[26] \Rightarrow 17x \equiv y - 5[26]$

$\Rightarrow 23(17x) \equiv 23(y - 5)[26]$

$\Rightarrow x \equiv 23y - 23 \times 5[26]$

$\Rightarrow x \equiv 23y + 15[26]$.

Réciproquement

$x \equiv 23y + 15[26] \Rightarrow 23y \equiv x - 15[26]$

$\Rightarrow 17(23y) \equiv 17(x - 15)[26]$

$\Rightarrow y \equiv 17x + 5[26]$.

Donc $y \equiv 17x + 5[26] \Leftrightarrow x \equiv 23y + 15[26]$.

iv. La fonction de décodage associée à $y \in E$, $x \in E$ tel que $x \equiv 23y + 15[26]$.

Avec le tableur :

$L' \mapsto \text{CODE}(L') - 65$
 $t \mapsto \text{MOD}(23*t + 15)$
 $u \mapsto \text{CAR}(u + 65) = L$

b. Le philosophe est CONDORCET.

Dans le codage du manuel il manque la lettre H à la fin du neuvième bloc. Cette erreur a été rectifiée dans la citation.

La citation est : « REJETER LA THÉORIE COMME INUTILE POUR NE S'APPLIQUER QU'AUX CHOSES USUELLES C'EST PROPOSER DE RETRANCHER LES RACINES D'UN ARBRE SOUS PRÉTEXTE QU'ELLES NE PORTENT POINT DE FRUITS »

(les espaces et les apostrophes ont été rajoutés)

3 a. E est codée par W se traduit par $4a + b \equiv 22[26]$.

A est codée par U se traduit par $0a + b \equiv 20[26]$.

On doit donc chercher a et b tels que

$\begin{cases} 4a + b \equiv 22[26] \\ b \equiv 20[26] \end{cases}$

$\begin{cases} 4a + b \equiv 22[26] \\ b \equiv 20[26] \end{cases}$

b.

x	0	1	2	3	4	5	6	7	8
4x	0	4	8	12	16	20	24	2	6
x	9	10	11	12	13	14	15	16	17
4x	10	14	18	22	0	4	8	12	16
x	18	19	20	21	22	23	24	25	
4x	20	24	2	6	10	14	18	22	

Il existe deux entiers naturels compris entre 0 et 25 tels que $4x \equiv 2 [26]$: $u = 7$ et $u = 20$ mais il y en a un seul qui donne « une bonne clé », c'est-à-dire qui code deux lettres distinctes par deux lettres distinctes : c'est $u = 7$, d'où $a = 7$ et $b = 20$.

c. La fonction de codage probable est $y \equiv 7x + 20 [26]$.

Exercices

Maîtriser le cours

1 Expressions synonymes de « b divise a » :
 a est un multiple de b ; a est divisible par b ;
 b est un diviseur de a .

2 Par hypothèse, il existe des entiers relatifs k et k' tels que $a = bk$ et $b = ck'$. D'où $a = c(k'k)$ et kk' étant un entier relatif, a est donc multiple de c .

3 Par hypothèse, il existe des entiers relatifs k et k' tels que $b = ak$ et $c = ak'$. D'où
 $bu + cv = aku + ak'v = a(ku + k'v)$ et $ku + k'v$
 étant un entier relatif, a divise donc $bu + cv$.

4 Effectuer la division euclidienne de l'entier relatif a par l'entier naturel non nul b , c'est déterminer des entiers q et r tels que $a = bq + r$ et $0 \leq r < b$.

5 Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Soient des entiers q, r, q' et r' vérifiant $a = bq + r = bq'r + r'$ et $0 \leq r < b$ et $0 \leq r' < b$. On a alors :
 $b(q - q') = r' - r$ et $-b < r' - r < b$. On en déduit $r' - r = 0$ (car 0 est le seul multiple de b compris strictement entre $-b$ et b), puis $b(q - q') = 0$ et $q - q' = 0$ (car $b \neq 0$).

6 Dire que a est congru à b modulo n c'est dire que a et b ont le même reste dans la division euclidienne par n , ou que $a - b$ est un multiple de n .

7 Voir cours page 20.

8 Voir cours page 20.

9 a. Faux (contre-exemple : 2 divise -2 et -2 divise 2)

b. Faux (contre-exemple : 2 divise 6 et 6 ne divise pas 2)

c. Vrai ($b = ak$ implique $bc = a(kc)$)

d. Faux (contre-exemple : 6 divise 4×3 mais 6 ne divise ni 4 ni 3).

e. Vrai ($b = ak$ implique $a + b = a(1 + k)$).

f. Vrai ($a + b = k'a$ implique $b = a(k' - 1)$)

g. Vrai (propriété 3)

h. Faux (contre-exemple : 6 divise 5 + 7 mais 6 ne divise ni 5 ni 7).

i. Faux (contre-exemple : 6 et 4 divisent 12 mais 6×4 ne divise pas 12).

j. Vrai ($b = ak$ implique $b^2 = a^2(k^2)$).

10 a. Faux ($17 > 15$)

b. Vrai.

c. Faux ($-17 < 0$)

d. Vrai ($-287 = 18 \times (-16) + 1$ et $0 \leq 1 < 18$)

e. Faux (contre-exemple pour $n = 3$: 9 n'est pas le reste de la division euclidienne de $11n^3 + 9$ par 3 ; $11n^3 + 9 = n(11n^2) + 9$ et la condition $0 \leq 9 < n$ n'est pas vérifiée pour tout entier naturel n non nul)

f. Faux ($a = bq + r$ et $0 \leq r < b$ implique $a + b = b(q + 1) + r$ et $0 \leq r < b$; donc le quotient est augmenté de 1 et le reste est inchangé)

g. Vrai.

h. Faux (le reste doit être positif)

i. Faux (contre-exemple : $14 = 3 \times 4 + 2$ et $14 + 1 = 3 \times 5 + 0$, donc 2 est le reste de la division euclidienne de 14 par 3 mais le reste de la division euclidienne de $14 + 1$ par 3 est 0 et non $2 + 1$)

j. Faux (contre-exemple : $0 \leq 5 < 6$, donc 5 est bien le reste de la division euclidienne de a par 6 mais la condition $0 \leq 5 < b$ n'est pas vérifiée pour $b = 4$).

11 Cet algorithme donne le quotient q et le reste r de la division euclidienne d'un entier relatif a par un entier naturel non nul b .

12 a. Faux (il peut être aussi congru à 0 modulo 5).

b. Faux (contre-exemple : 17 est congru à 12 modulo 5 mais 12 n'est pas le reste de la division euclidienne de 17 par 5).

c. Vrai.

d. Faux ($244 - 205 = 39$, donc la 2^e congruence est vraie mais la 1^e est fausse car $257 - 10 = 247$ n'est pas un multiple de 9).

e. Vrai.

f. Vrai ($19 \equiv 1 [18]$ d'où $19^n \equiv 1 [18]$, soit $19^n - 1$ est divisible par 18).

g. Faux ($4 \equiv 1 [3]$ et $2 \equiv -1 [3]$, d'où $4^n \equiv 1 [3]$ et $2^n \equiv (-1)^n [3]$ et par somme $4^n + 2^n \equiv 1 + (-1)^n [3]$ or $1 + (-1)^n \equiv 0 [3]$ si et seulement si n est impair).

h. Vrai ($a \equiv 3 [7]$ et $b \equiv 5 [7]$ impliquent $3a \equiv 9 [7]$ soit $3a \equiv 2 [7]$ et $8b \equiv 5 [7]$, d'où par somme $3a + 8b \equiv 2 + 5 [7]$ soit $3a + 8b \equiv 0 [7]$).

i. Faux (contre-exemple : $2 \times 10 \equiv 2 \times 12 [4]$, mais 10 n'est pas congru à 12 modulo 4).

j. Vrai ($a \equiv b [6]$ alors $a - b = 6k$ ($k \in \mathbb{Z}$), d'où $a - b = 3(2k)$ et $a \equiv b [3]$).

k. Vrai ($2a \equiv 2b [2n]$ signifie $2a - 2b = 2nk$ ($k \in \mathbb{Z}$), d'où en simplifiant par 2 non nul, $a - b = nk$, soit $a \equiv b [n]$).

Appliquer les capacités attendues

14 a. Les multiples n de 17 sont de la forme $n = 17k$ ($k \in \mathbb{Z}$). Pour k entier relatif, $2\,000 \leq 17k \leq 3\,000$ équivaut à $118 \leq k \leq 176$. Il y a donc $176 - 118 + 1 = 59$ multiples de 17 compris entre 2000 et 300.

b. De même, pour k entier relatif, $-1\,000 \leq 41k \leq 2\,000$ équivaut à $-24 \leq k \leq 48$. Il y a donc $48 - (-24) + 1 = 73$ multiples de 41 compris entre -1 000 et 2 000.

15 a. 11 divise $n + 5$ si et seulement si il existe un entier relatif k tel que $n + 5 = 11k$, soit $n = -5 + 11k$ ou si et seulement si il existe un entier relatif k' tel que $n = 6 + 11k'$.

b. Les diviseurs de 11 sont -1, 1, -11 et 11. $n + 5$ divise 11 si et seulement si $n + 5 = -1$ ou $n + 5 = 1$ ou $n + 5 = 11$ ou $n + 5 = -11$, soit $n = -6$ ou $n = -4$ ou $n = 6$ ou $n = -16$.

16 Les diviseurs de 10 sont : -1, 1, -2, 2, -5, 5, -10 et 10. Ainsi $2n + 3$ divise 10 si et seulement si : $2n + 3 = -1$ ou $2n + 3 = 1$ ou $2n + 3 = -2$ ou $2n + 3 = 2$ ou $2n + 3 = -5$ ou $2n + 3 = 5$ ou $2n + 3 = -10$ ou $2n + 3 = 10$, soit $2n = -4$ ou $2n = -2$ ou $2n = -5$ ou $2n = -1$ ou $2n = -8$ ou $2n = 2$ ou $2n = -13$ ou $2n = 7$, soit $n = -2$ ou $n = -1$ ou $n = -4$ ou $n = 1$.

17 Soient n et n' des entiers pairs, il existe alors des entiers k et k' tels que $n = 2k$ et $n' = 2k'$, d'où $n + n' = 2(k + k')$.

Soient n et n' des entiers impairs, il existe alors des entiers k et k' tels que $n = 2k + 1$ et $n' = 2k' + 1$, d'où $n + n' = 2(k + k' + 1)$. La somme de deux entiers de même parité est donc paire.

18 Soient n et n' deux entiers impairs consécutifs, il existe donc un entier relatif k tel que $n = 2k + 1$ et $n' = 2k + 3$, d'où $n + n' = 4k + 4 = 4(k + 1)$. Donc, la somme $n + n'$ est un multiple de 4.

20 Si $2n - 5$ divise $n + 3$ alors $2n - 5$ divise $2(n + 3) - (2n - 5) = 11$, d'où $2n - 5 = -1$ ou $2n - 5 = 1$ ou $2n - 5 = -11$ ou $2n - 5 = 11$, soit $n = -3$ ou $n = 2$ ou $n = 3$ ou $n = 8$. Réciproquement : si $n = -3$ alors $2n - 5 = -11$ et $n + 3 = 0$; si $n = 2$ alors $2n - 5 = -1$ et $n + 3 = 5$; si $n = 3$ alors $2n - 5 = 1$ et $n + 3 = 4$; si $n = 8$ alors $2n - 5 = 11$ et $n + 3 = 11$. Dans tous les cas $2n - 5$ divise $n + 3$. Il y a donc 4 solutions : -3, 2, 3 et 8.

21 Si $n - 3$ divise $2n + 12$ alors $n - 3$ divise $2n + 12 - 2(n - 3) = 18$ et réciproquement si $n - 3$ divise 18 alors $n - 3$ divise $2(n - 3) + 18 = 2n + 12$. Donc $n - 3$ divise $2n + 12$ si et seulement si $n - 3$ divise 18. Les diviseurs de 18 étant -18, -9, -6, -3, -2, -1, 1, 2, 3, 6, 9, 18, les solutions sont donc : -15, -6, -3, 0, 1, 2, 4, 5, 6, 9, 12, 21.

22 Si $3n + 7$ divise $5n + 15$, alors $3n + 7$ divise $3(5n + 15) - 5(3n + 7) = 10$. Les diviseurs de 10 étant -10, -5, -2, -1, 1, 2, 5, 10 on en déduit : $3n + 7 = -10$ ou $3n + 7 = -5$ ou $3n + 7 = -2$ ou $3n + 7 = -1$ ou $3n + 7 = 1$ ou $3n + 7 = 2$ ou $3n + 7 = 5$ ou $3n + 7 = 10$, soit $n = -4$ ou $n = -3$ ou $n = -2$ ou $n = 1$.

Réciproquement : si $n = -4$ alors $3n + 7 = -5$ et $5n + 15 = -5$ et -5 divise -5; si $n = -3$ alors $3n + 7 = -2$ et $5n + 15 = 0$ et -2 divise 0; si $n = -2$ alors $3n + 7 = 1$ et $5n + 15 = 5$ et 1 divise 5; si $n = 1$ alors $3n + 7 = 10$ et $5n + 15 = 20$ et 10 divise 20. Il y a donc quatre solutions : -4, -3, -2 et 1.

23 Si a divise $15n + 2$ et $10n + 7$, alors a divise $3(10n + 7) - 2(15n + 2) = 17$.

24 Dans cet exercice on veut montrer que 1 et 3 sont les seuls diviseurs possibles de $5n + 29$ et $2n + 11$.

Soit d un diviseur positif de $5n + 29$ et $2n + 11$, alors d divise $2(5n + 29) - 5(2n + 11) = 3$, donc $d = 1$ ou $d = 3$. Les seuls diviseurs positifs possibles sont 1 et 3.

On peut chercher quels sont les entiers naturels n pour lesquels 3 divise $5n + 29$ et $2n + 11$:

Si 3 divise $5n + 29$ et $2n + 11$ alors 3 divise $5n + 29 - 2(2n + 11) = n + 7$, soit $n = -7 + 3k$, soit $n = 2 + 3k'$.

Réciproquement si $n = 2 + 3k'$ ($k' \in \mathbb{N}$), alors 3 divise $5(2 + 3k') + 29$ et $2(2 + 3k') + 11$.

3 divise $5n + 29$ et $2n + 11$ si et seulement si $n = 2 + 3k'$.

Donc si $n = 2 + 3k'$ alors $5n + 29$ et $2n + 11$ admettent comme seuls diviseurs positifs communs 1 et 3 ; sinon $5n + 29$ et $2n + 11$ ont 1 pour seul diviseur positif commun.

25 b. Si $n - 2$ divise $n^2 - 5n + 11$ alors $n - 2$ divise $n^2 - 5n + 11 - (n - 2)(n - 3) = 5$, d'où $n - 2 = -5$ ou $n - 2 = -1$ ou $n - 2 = 1$ ou $n - 2 = 5$, soit $n = -3$ ou $n = 1$ ou $n = 3$ ou $n = 7$. Réciproquement si $n = 1$ alors $n - 2 = -1$ et -1 divise $n^2 - 5n + 11$; si $n = 3$ alors $n - 2 = 1$ et 1 divise $n^2 - 5n + 11$; si $n = 7$ alors $n - 2 = 5$ et $n^2 - 5n + 11 = 25$ et 5 divise 25. Les solutions sont donc : 1, 3 et 7.

27 • Pour $n = 0$, $5^{2n} + 3 = 4$. La propriété est donc vraie pour $n = 0$.

• On montre que si la propriété est vraie à un rang n alors elle est vraie au rang $n + 1$.

$5^{2(n+1)} + 3 = 5^{2n} \times 5^2 + 3 = (5^{2n} + 3)5^2 - 3 \times 5^2 + 3 = (5^{2n} + 3)5^2 - 3 \times 24$. Or 4 divise $5^{2n} + 3$ par hypothèse de récurrence et 4 divise 24, d'où 4 divise $(5^{2n} + 3)5^2 - 3 \times 24$. La propriété est donc vraie au rang $n + 1$. Par récurrence, elle est vraie pour tout $n \in \mathbb{N}$.

28 b. $19^n - 12^n = (19 - 12)(19^{n-1} + 19^{n-2} \times 12 + \dots + 19 \times 12^{n-2} + 12^{n-1})$, d'où $19^n - 12^n = 7k$ (k entier naturel).

c. Pour $n = 1$, $19^n - 12^n = 7$. La propriété est donc vraie pour $n = 1$.

On démontre que si la propriété est vraie à un rang n non nul, alors elle est vraie au rang $n + 1$.

$19^{n+1} - 12^{n+1} = 19^n \times 19 - 12^n \times 12 = 19^n(19 - 12) + 19^n \times 12 - 12^n \times 12 = 19^n \times 7 + 12(19^n - 12^n)$. Or 7 divise $19^n - 12^n$ par hypothèse de récurrence, donc 7 divise $19^n \times 7 + 12(19^n - 12^n)$. La propriété est donc vraie au rang $n + 1$. On conclut d'après le principe de récurrence.

29 Pour $n = 0$, $5^{2n} - 2^{3n} = 1 - 1 = 0$. La propriété est donc vraie.

On montre que si la propriété est vraie au rang n alors elle est vraie au rang $n + 1$.

$5^{2(n+1)} - 2^{3(n+1)} = 5^{2n} \times 25 - 2^{3n} \times 8 = (5^{2n} - 2^{3n}) \times 25 + 2^{3n} \times 25 - 2^{3n} \times 8 = 25(5^{2n} - 2^{3n}) + 2^{3n} \times 17$. Or 17 divise $5^{2n} - 2^{3n}$, donc 17 divise $17 \times 2^{3n} + 25(5^{2n} - 2^{3n})$. La propriété est donc vraie à l'ordre $n + 1$. On conclut d'après le principe de récurrence.

30 Pour $n = 0$, $5n^3 + n = 0$. La propriété est donc vraie.

On montre que si la propriété est vraie au rang n alors elle est vraie au rang $n + 1$.

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

Or 6 divise $5n^3 + n$, par hypothèse de récurrence, et $15n(n + 1) = 6(5k)$ car $n(n + 1) = 2k$. On en déduit alors que 6 divisant les 3 termes divise la somme. La propriété est donc vraie au rang $n + 1$. On conclut d'après le principe de récurrence.

32 $x^2 = y^2 + 13 \Leftrightarrow x^2 - y^2 = 13 \Leftrightarrow (x - y)(x + y) = 13$.

Soit $(x ; y)$ un couple d'entiers relatifs solution, on en déduit que $(x - y)$ et $(x + y)$ sont deux diviseurs associés de 13. D'où :

$$\begin{cases} x - y = -1 \\ x + y = -13 \end{cases} \text{ ou } \begin{cases} x - y = -13 \\ x + y = -1 \end{cases} \text{ ou } \begin{cases} x - y = 1 \\ x + y = 13 \end{cases} \text{ ou } \begin{cases} x - y = 13 \\ x + y = 1 \end{cases}, \text{ soit :}$$

$(x ; y) = (-7 ; -6)$ ou $(x ; y) = (-7 ; 6)$ ou

$(x ; y) = (7 ; 6)$ ou $(x ; y) = (7 ; -6)$.

On vérifie que ces couples sont solutions.

Il y a donc quatre couples solutions.

33 $4x^2 = y^2 + 15 \Leftrightarrow 4x^2 - y^2 = 15$
 $\Leftrightarrow (2x - y)(2x + y) = 15$.

Soit $(x ; y)$ un couple d'entiers naturels solution, on en déduit que $2x - y$ et $2x + y$ sont des diviseurs associés de 15. On remarque que x et y étant entiers naturels, $2x + y$ est un entier naturel de même que $2x - y$, puisque $(2x - y)(2x + y) = 15$ et enfin que $2x - y < 2x + y$. Donc $2x - y$ et $2x + y$ sont deux diviseurs associés positifs de 15 tels que $2x - y < 2x + y$. On déduit :

$$\begin{cases} 2x - y = 1 \\ 2x + y = 15 \end{cases} \text{ ou } \begin{cases} 2x - y = 3 \\ 2x + y = 5 \end{cases}$$

soit $(x ; y) = (4 ; 7)$ ou $(x ; y) = (2 ; 1)$.

On vérifie que ces deux couples sont solutions.

34 $3xy - y^2 = 25 \Leftrightarrow y(3x - y) = 25$.

Soit $(x ; y)$ un couple d'entiers relatifs solution, on en déduit que y et $3x - y$ sont des diviseurs associés de 25, d'où :

$$\begin{cases} y = -1 \\ 3x - y = -25 \end{cases} \text{ ou } \begin{cases} y = -25 \\ 3x - y = -1 \end{cases} \text{ ou}$$

$$\begin{cases} y = 1 \\ 3x - y = 25 \end{cases} \text{ ou } \begin{cases} y = 25 \\ 3x - y = 1 \end{cases} \text{ ou } \begin{cases} y = -5 \\ 3x - y = -5 \end{cases} \text{ ou } \begin{cases} y = 5 \\ 3x - y = 5 \end{cases}$$

Aucun de ces systèmes n'a de solution entière. L'équation n'a donc pas de solution entière.

35 $36 + x^2$ est le carré d'un entier si et seulement s'il existe un entier naturel y tel que $36 + x^2 = y^2$. Le problème revient à trouver des couples $(x; y)$ d'entiers naturels tels que $y^2 - x^2 = 36$, soit $(y - x)(y + x) = 36$. En raisonnant comme dans l'exercice 33 et en remarquant que la somme et la différence de deux entiers sont de même parité, on obtient que :

$$\begin{cases} y - x = 2 \\ y + x = 18 \end{cases} \text{ ou } \begin{cases} y - x = 6 \\ y + x = 6 \end{cases} \text{ soit :}$$

$(x; y) = (8; 10)$ ou $(x; y) = (0; 6)$.

Il y a donc deux solutions 0 et 8.

37 On raisonne par l'absurde : s'il existait un couple d'entiers relatifs tel que $3x + 24y = 14$, 3 divisant $3x + 24y$ devrait diviser 14, ce qui est faux. L'équation n'a donc pas de solution dans $\mathbb{Z}$.

39 b. Pour $n \neq -4$

$$\frac{2n^2 - n - 8}{n + 4} = \frac{(n + 4)(2n - 9)}{n + 4} + \frac{28}{n + 4}$$

$$= 2n - 9 + \frac{28}{n + 4}.$$

Donc $\frac{2n^2 - n - 8}{n + 4}$ est un entier si et seulement si

$$\frac{28}{n + 4} \text{ est un entier.}$$

c. Pour $n \neq -4$, $\frac{28}{n + 4}$ est un entier si et seulement

si $n + 4$ divise 28, soit $n + 4 = -28$ ou $n + 4 = -14$ ou $n + 4 = -7$ ou $n + 4 = -4$ ou $n + 4 = -2$ ou $n + 4 = -1$ ou $n + 4 = 1$ ou $n + 4 = 2$ ou $n + 4 = 4$ ou $n + 4 = 7$ ou $n + 4 = 14$ ou $n + 4 = 28$. Les solutions sont : $-32, -18, -11, -8, -6; -5, -3, -2, 0, 3, 10$ et 24.

41 $121 = 23 \times 5 + 6$ et $0 \leq 6 < 23$.

D'où $-121 = 23 \times (-5) - 6$ soit $-121 = 23 \times (-6) + 23 - 6$.

Donc $-121 = 23 \times (-5) + 17$ et $0 \leq 17 < 23$.

42 Par hypothèse :

$$a = 225 \times q + 136 \text{ et } 0 \leq 136 < 225.$$

a. On en déduit :

$$a = 75 \times (3q) + 75 + 61, \text{ d'où } a = 75(3q + 1) + 61 \text{ et } 0 \leq 61 < 75.$$

b. $a = 45 \times (5q) + 45 \times 3 + 1$, soit

$$a = 45(5q + 3) + 1 \text{ et } 0 \leq 1 < 45.$$

c. $a = 9 \times (25q) + 9 \times 15 + 1$, soit

$$a = 9(25q + 15) + 1 \text{ et } 0 \leq 1 < 9.$$

$$\begin{cases} a = 13q + 9 \\ a = 15q + 1 \end{cases} \Leftrightarrow \begin{cases} a = 61 \\ q = 4 \end{cases}$$

$$\begin{cases} a + b = 324 \\ a = 2b + 57 \end{cases} \Leftrightarrow \begin{cases} b = 89 \\ a = 235 \end{cases}$$

Et $235 = 89 \times 2 + 57$ et $0 \leq 57 < 89$.

$$\begin{cases} a - b = 779 \\ a = 11b + 49 \end{cases} \Leftrightarrow \begin{cases} a = 852 \\ b = 73 \end{cases}$$

47 $a = 11q + 8$ et $0 \leq 8 < 11$.

$$b = 11q' + 3 \text{ et } 0 \leq 3 < 11.$$

a. On a alors $a + b = 11(q + q') + 11 =$

$$11(q + q' + 1) + 0;$$

$a + b$ est donc divisible par 11.

b. $a^2 = (11q + 8)^2 = 11(11q^2 + 16q + 5) + 9$ et

$0 \leq 9 < 11$, le reste est donc 9.

49 $85 = bq + 3$ et $0 \leq 3 < b$.

$$bq = 82 \text{ et } b > 3. \text{ D'où } b = 41 \text{ et } q = 2 \text{ ou } b = 82$$

et $q = 1$.

50 $a = b \times 100 + 13$ et $0 \leq 13 < b$ et $a < 900$.

Donc $100b + 13 < 900$, soit $100b < 887$, soit $b < 9$.

Or $b > 13$. Une telle division n'existe pas.

52 $2\,843 = 12 \times 236 + 11$ et $0 \leq 11 < 12$.

$$\text{D'où } \frac{2\,843}{6} \pi = \frac{12 \times 236 + 11}{6} \pi = 2 \times 236 \pi + \frac{11}{6} \pi.$$

53 $-3\,749 = 8 \times (-469) + 3$ et $0 \leq 3 < 8$. D'où

$$-\frac{3\,749}{4} \pi = \frac{8 \times (-469) + 3}{4} \pi = 2(-469) \pi + \frac{3\pi}{4}.$$

La mesure principale est donc $\frac{3\pi}{4}$.

$$\textbf{55} \quad 9n + 17 = (2n + 3) \times 4 + (n + 5) \text{ et}$$

$$0 \leq n + 5 < 2n + 3 \Leftrightarrow n > 2.$$

Donc si $n > 2$, dans la division euclidienne de $9n + 17$ par $2n + 3$, le quotient est 4 et le reste est $n + 5$.

Si $n = 0$ alors $17 = 3 \times 5 + 2$

Si $n = 1$ alors $26 = 5 \times 5 + 1$

Si $n = 2$ alors $35 = 7 \times 5 + 0$.

57 Il y a trois cas possibles : soit $n = 3k$, soit

$n = 3k + 1$, soit $n = 3k + 2$ (k entier naturel).

Si $n = 3k$, alors $n(n + 5)(n + 7) =$

$$3k(3k + 5)(3k + 7) = 3K.$$

Si $n = 3k + 1$, alors $n(n + 5)(n + 7) =$

$$(3k + 1)(3k + 6)(3k + 8) = 3K'.$$

Si $n = 3k + 2$, alors $n(n + 5)(n + 7) =$

$$(3k + 2)(3k + 7)(3k + 9) = 3K''.$$

Dans tous les cas, $n(n + 5)(n + 7)$ est un multiple de 3.

58 Il y a quatre cas possibles : soit $n = 4k$,

soit $n = 4k + 1$, soit $n = 4k + 2$, soit $n = 4k + 3$

(k entier naturel).

Si $n = 4k$ alors $n(n + 5)(n + 7) =$

$$4k(4k + 5)(4k + 7) = 4K.$$

Si $n = 4k + 1$ alors $n(n + 5)(n + 7) =$

$$(4k + 1)(4k + 6)(4k + 8) = 4K'.$$

Si $n = 4k + 2$ alors $n(n + 5)(n + 7) =$

$$(4k + 2)(4k + 7)(4k + 9) = 4K'' + 4 \times 31 + 2.$$

Si $n = 4k + 3$ alors $n(n+5)(n+7) = (4k+3)(4k+8)(4k+10) = 8K'''$.

Dans tous les cas $n(n+5)(n+7)$ est un multiple de 2. Par contre $n(n+5)(n+7)$ est un multiple de 4 si et seulement si le reste de la division de n par 4 n'est pas égal à 2.

59 a. Les restes possibles de la division euclidienne de n par 5 sont : 0 ou 1 ou 2 ou 3 ou 4, cela signifie que $n = 5k$ ou $n = 5k + 1$ ou $n = 5k + 2$ ou $n = 5k + 3$ ou $n = 5k + 4$.

b. On fait une étude exhaustive :

- Si $n = 5k$ alors $n^2 - 3n + 6 = 5(5k^2 - 3k + 1) + 1$, donc $r = 1$; si $n = 5k + 1$ alors $n^2 - 3n + 6 = (5k + 1)^2 - 3(5k + 1) + 6 = 5K + 1 - 3 + 6 = 5K + 4$, donc $r = 4$;

- si $n = 5k + 2$ alors $n^2 - 3n + 6 = (5k + 2)^2 - 3(5k + 2) + 6 = 5K' + 4 - 6 + 6 = 5K' + 4$, donc $r = 4$;

- si $n = 5k + 3$ alors $n^2 - 3n + 6 = (5k + 3)^2 - 3(5k + 3) + 6 = 5K'' + 9 - 9 + 6 = 5(K'' + 1) + 1$, donc $r = 1$;

- si $n = 5k + 4$ alors $n^2 - 3n + 6 = (5k + 4)^2 - 3(5k + 4) + 6 = 5K''' + 16 - 12 + 6 = 5(K''' + 2)$, donc $r = 0$.

Donc $n^2 - 3n + 6$ est divisible par 5 si et seulement si $n = 5k + 4$.

60 On fait une étude suivant les congruences modulo 5 de n .

Si $n \equiv 0 [5]$ alors $n^2 \equiv 0^2 [5]$, soit $n^2 \equiv 0 [5]$;

Si $n \equiv 1 [5]$ alors $n^2 \equiv 1^2 [5]$, soit $n^2 \equiv 1 [5]$;

Si $n \equiv 2 [5]$ alors $n^2 \equiv 2^2 [5]$, soit $n^2 \equiv 4 [5]$, soit $n \equiv -1 [5]$;

Si $n \equiv 3 [5]$ alors $n^2 \equiv 3^2 [5]$, soit $n^2 \equiv 9 [5]$, soit $n \equiv -1 [5]$;

Si $n \equiv 4 [5]$ alors $n^2 \equiv 4^2 [5]$, soit $n^2 \equiv 16 [5]$, soit $n \equiv 1 [5]$.

Donc $n^2 \equiv 0 [5]$ ou $n^2 \equiv -1 [5]$ ou $n^2 \equiv 1 [5]$. Donc $n^2 = 5q$ ou $n^2 = 5q + 1$ (q entier naturel) ou $n^2 = 5q - 1$ (q entier naturel non nul).

61 On montre que pour tout entier n , $n^2 \equiv 0 [4]$ ou $n^2 \equiv 1 [4]$. Donc si un entier x est somme de deux carrés, on a nécessairement : $x \equiv 0 + 0 [4]$ ou $x \equiv 1 + 1 [4]$ ou $x \equiv 1 + 0 [4]$.

x étant de plus impair, on a $x \equiv 1 [4]$, soit x est de la forme $x = 1 + 4k$ (k entier relatif).

63 Dans cet exercice on cherche à déterminer b tel que $b \equiv a [7]$ et $-3 \leq b \leq 3$.

a. $13 \equiv 13 - 2 \times 7 [7]$, d'où $a \equiv -1 [7]$ et $-3 \leq -1 \leq 3$ et $b = -1$.

b. $19 \equiv 19 - 3 \times 7 [7]$, d'où $a \equiv -2 [7]$ et $-3 \leq -2 \leq 3$ et $b = -2$.

c. $64 \equiv 9 \times 7 + 1$, d'où $64 \equiv 1 [7]$ et $-3 \leq 1 \leq 3$ et $b = 1$.

d. $88 \equiv 13 \times 7 - 3$, d'où $88 \equiv -3 [7]$ et $-3 \leq -3 \leq 3$ et $b = -3$.

e. $-6 \equiv -6 + 7 [7]$, d'où $b = 1$.

f. $-4 \equiv -4 + 7 [7]$, d'où $b = 3$.

65 a. $16 \equiv 2 [14]$, d'où $16^{31} \equiv 2^{31} [14]$, d'où $16^{31} - 2^{31} \equiv 0 [14]$.

b. $13 \equiv 2 [11]$, d'où $13^{20} \equiv 2^{20} [11]$;

$9 \equiv -2 [11]$, d'où $9^{20} \equiv (-2)^{20} [11]$;

En retranchant les congruences membre à membre, on obtient : $13^{20} - 9^{20} \equiv 2^{20} - (-2)^{20} [11]$.

d'où $13^{20} - 9^{20} \equiv 0 [11]$.

66 $a \equiv 3 [5] \Rightarrow a^2 \equiv 3^2 [5] \Rightarrow a^2 \equiv -1 [5]$, d'où

$7a^2 \equiv -7 [5] \text{ (c1)} ;$

$b \equiv 4 [5] \Rightarrow b^2 \equiv 4^2 [5] \Rightarrow b^2 \equiv 1 [5]$, d'où

$4b^2 \equiv 4 [5] \text{ (c2)} ;$

De (c1) et (c2) on déduit : $7a^2 + 4b^2 \equiv -7 + 4 [5]$, soit

$7a^2 + 4b^2 \equiv 2 [5]$ et $0 \leq 2 < 5$, d'où le reste $r = 2$.

67 a. $2012 \equiv 2 [5] \Rightarrow 2012^{2011} \equiv 2^{2011} [5]$.

$2^2 \equiv -1 [5] \Rightarrow (2^2)^2 \equiv (-1)^2 [5] \Rightarrow 2^4 \equiv 1 [5]$.

Or $2011 = 4 \times 502 + 3$, d'où $2^{2011} = (2^4)^{502} \times 2^3$.

$2^4 \equiv 1 [5] \Rightarrow (2^4)^{502} \equiv 1^{502} [5] \Rightarrow (2^4)^{502} \times 2^3 \equiv 2^3 [5]$ soit $2^{2011} \equiv 3 [5]$, donc $2012^{2011} \equiv 3 [5]$ et $0 \leq 3 < 5$

b. $2012 = 7 \times 287 + 3$, donc $2012 \equiv 3 [7]$, d'où $2012^{2011} \equiv 3^{2011} [7]$. Or $3^3 \equiv -1 [7] \Rightarrow 3^6 \equiv 1 [7]$

et $2011 = 6 \times 335 + 1$, d'où $3^{2011} = (3^6)^{335} \times 3$.

On en déduit $3^{2011} \equiv 1^{335} \times 3 [7]$ et $2012^{2011} \equiv 3 [7]$.

D'où le reste $r = 3$.

68 a. $7^2 = 49$, d'où $7^2 \equiv -1 [5]$.

b. De **a.** on déduit $(7^2)^2 \equiv (-1)^2 [5]$ soit $7^4 \equiv 1 [5]$

c. De **b.** on déduit, pour tout entier naturel k : $(7^4)^k \equiv 1^k [5]$ soit $7^{4k} \equiv 1 [5]$.

d. De **c.** on déduit successivement

$7^{4k} \times 7 \equiv 7 [5]$ soit $7^{4k+1} \equiv 2 [5]$

$7^{4k} \times 7^2 \equiv -1 [5]$ soit $7^{4k+2} \equiv 4 [5]$

$7^{4k+2} \times 7 \equiv -7 [5]$ soit $7^{4k+3} \equiv -2 [5]$ soit $7^{4k+3} \equiv 3 [5]$

e. On note r le reste de la division euclidienne de 7^n par 5. D'après **d.** :

si $n = 4k$ alors $r = 1$; si $n = 4k + 1$ alors $r = 2$; si $n = 4k + 2$ alors $r = 4$ et si $n = 4k + 3$ alors $r = 3$.

69 a. Dans la division euclidienne par 5 les restes possibles sont : 0 ou 1 ou 2 ou 3 ou 4. Donc pour tout entier x :

$x \equiv 0 [5]$ ou $x \equiv 1 [5]$ ou $x \equiv 2 [5]$ ou $x \equiv 3 [5]$ ou

$x \equiv 4 [5]$ ce qui équivaut à $x \equiv 0 [5]$ ou $x \equiv 1 [5]$

ou $x \equiv 2 [5]$ ou $x \equiv -2 [5]$ ou $x \equiv -1 [5]$

b. et c.

$x \bmod 5$	-2	-1	0	1	2
$x^2 \bmod 5$	4	1	0	1	4
$x^4 \bmod 5$	1	1	0	1	1

d. On note r le reste de la division euclidienne de x^4 par 5. Si $x \equiv 0 [5]$ alors $r = 0$, sinon $r = 1$.

70 a.

$n \bmod 5$	-2	-1	0	1	2
$n^2 \bmod 5$	-1	1	0	1	-1
$-3n \bmod 5$	1	-2	0	2	-1
$n^2 - 3n + 6 \bmod 5$	1	0	1	-1	-1

b. Avec les mêmes notations que pour l'exercice précédent :

si $n \equiv 0 [5]$ alors $r = 1$; si $n \equiv 1 [5]$ alors $r = 4$;

si $n \equiv 2 [5]$ alors $r = 4$; si $n \equiv 3 [5]$ alors $r = 1$;

si $n \equiv 4 [5]$ alors $r = 0$.

72 a.

$x \bmod 7$	0	1	2	3	4	5	6
$4x \bmod 7$	0	4	1	5	2	6	3

b. Par disjonction des cas, on déduit de **a.** que $4x \equiv 6 [7]$ si et seulement si $x \equiv 5 [7]$. Les solutions sont donc les entiers x de la forme $x = 5 + 7k$ (k entier relatif).

73 1. a. $7x \equiv 3 [11] \Rightarrow 8 \times 7x \equiv 8 \times 3 [11] \Rightarrow 56x \equiv 24 [11]$;

or $56 \equiv 1 [11] \Rightarrow 56x \equiv x [11]$ et $24 \equiv 2 [11]$, donc $7x \equiv 3 [11] \Rightarrow x \equiv 2 [11]$.

Réciproquement si $x \equiv 2 [11]$ alors $7x \equiv 14 [11]$, soit $7x \equiv 3 [11]$. Donc $7x \equiv 3 [11] \Leftrightarrow x \equiv 2 [11]$.

Les solutions sont donc les entiers x de la forme $x = 2 + 11k$ (k entier relatif).

(On peut aussi raisonner comme dans l'exercice 72).

b. $7x \equiv 3 [10] \Rightarrow 3 \times 7x \equiv 9 [10] \Rightarrow x \equiv 9 [10]$;

Réciproquement :

$x \equiv 9 [10] \Rightarrow 7x \equiv 7 \times 9 [10] \Rightarrow 7x \equiv 3 [10]$.

Donc $7x \equiv 3 [10] \Leftrightarrow x \equiv 9 [10]$. Les solutions sont les entiers de la forme $9 + 10k$ (k entier relatif).

c.

$x \bmod 10$	0	1	2	3	4	5	6	7	8	9
$5x \bmod 10$	0	5	0	5	0	5	0	5	0	5

On constate que pour tout entier x , $5x$ est congru à 0 ou 5 modulo 10, donc il n'existe pas d'entier x tel que $5x \equiv 3 [10]$.

d. D'après l'étude exhaustive précédente $5x \equiv 0 [10]$ si et seulement si x est pair.

2. a. $5x + 25 \equiv 56 [7] \Leftrightarrow 5x + 4 \equiv 0 [7]$

$$\Leftrightarrow 5x \equiv -4 [7]$$

$$\Leftrightarrow 5x \equiv 3 [7].$$

Or $5x \equiv 3 [7] \Rightarrow 3(5x) \equiv 9 [7] \Rightarrow x \equiv 2 [7]$.

Réciproquement $x \equiv 2 [7] \Rightarrow 5x \equiv 10 [7] \Rightarrow 5x \equiv 3 [7]$.

Donc $5x \equiv 3 [7] \Leftrightarrow x \equiv 2 [7]$.

Les solutions sont les entiers de la forme $2 + 7k$ (k entier relatif).

b. $8x - 23 \equiv 5x - 45 [17] \Leftrightarrow 8x - 6 \equiv 5x + 6 [17]$;

$$\Leftrightarrow 3x \equiv 12 [17].$$

Or $3x \equiv 12 [17] \Rightarrow 6(3x) \equiv 72 [17] \Rightarrow x \equiv 4 [17]$.

Réciproquement : si $x \equiv 4 [17] \Rightarrow 3x \equiv 12 [17]$;

donc $3x \equiv 12 [17] \Leftrightarrow x \equiv 4 [17]$.

Les solutions sont les entiers de la forme $4 + 17k$ (k entier relatif).

75 a. $5 \equiv 0 [5] \Rightarrow 5y^2 \equiv 0 [5] \Rightarrow 3x^2 + 5y^2 \equiv 3x^2 [5]$.

Or si $(x; y)$ est solution de $3x^2 + 5y^2 \equiv 16 [5]$, alors $3x^2 \equiv 16 [5]$ soit $3x^2 \equiv 1 [5]$.

b.

$x \bmod 5$	0	1	2	3	4
$x^2 \bmod 5$	0	1	4	4	1
$3x^2 \bmod 5$	0	3	2	2	3

On constate que $3x^2$ n'est pas congru à 1 modulo 5, donc la congruence $3x^2 \equiv 1 [5]$ n'a pas de solution et donc l'équation $3x^2 + 5y^2 = 16$ n'a pas de solution.

76

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

77

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

S'entraîner

78 a. n impair signifie que $n = 2k + 1$ ($k \in \mathbb{N}$), donc $n^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$ et $k(k + 1) = 2s$ est pair donc $n^2 - 1 = 8s$ est pair aussi.

b. Si $n = 2k$, $n^2 = 4k^2$

c. Si n est pair, n^2 est pair. Si n est impair, n^2 est impair donc par contraposée, si n^2 est pair, n est pair.

79 a. $0 = n^2 - 5n + 56 = n(n - 5) + 56 \Leftrightarrow n(n - 5) = 56$.

b. $S - (S - n) = n$ donc $n(S - n) = (S - n)(S - (S - n))$.

c. n et $S - n$ sont des diviseurs associés de 56.

$56 = 1 \times 56 = 2 \times 28 = 4 \times 14 = 7 \times 8$ donc

$S \in \{57, 30, 18, 15\}$

80 a. Si l'entier a est une solution de (E), $a(a^2 + a + b) = -c$, alors a divise c .

b. Si a est solution, a divise 3, donc $a \in \{-3, -1, 1, 3\}$. Aucune des valeurs ne convient, donc l'équation n'a pas de solution.

c. Toute solution entière divise 4. Seule la valeur 4 convient.

81 a. $56 = 1 \times 56 = 2 \times 28 = 4 \times 14 = 7 \times 8$.

b. Si b divise a , alors b divise $a - 2b = 56$ donc $n + 7 \in \{1, 2, 7, 8, 14, 28, 56\}$ donc $n \in \{0, 1, 7, 21, 49\}$.

Réciproquement, ces nombres conviennent.

82 a. $2n + 16 = 2k(2n - 5)$ donc

$2n - 5$ divise $2n + 16 - (2n - 5) = 21$, donc

$2n - 5 \in \{-21, -7, -3, -1, 1, 3, 7, 21\}$ donc

$n \in \{-8, -1, 1, 2, 3, 4, 6, 13\}$

b. Toutes ces valeurs conviennent.

83 $(n + 2)^3 = n^3 + 6n^2 + 12n + 8 = n^2(n + 6) + 12n + 8$.

$12n + 8$ est le reste dans la division de $(n + 2)^3$ par n^2 si $0 \leq 12n + 6 < n^2$ donc si $n \geq 0$ et $n^2 - 12n - 8 \leq 0$ alors $n \leq 12$.

84 $x^2 \equiv 1 [2]$ donc x^2 impair donc x est impair.

On a $x = 2p + 1$. Si $y = 2q + 1$, alors

$x^2 - 2y^2 = 4p^2 + 4p + 1 - 8q^2 - 8q - 2 =$

$4(p^2 + p - 2q^2 - 2q) - 1$

donc $x^2 - 2y^2 = 1 \Leftrightarrow 4(p^2 + p - 2q^2 - 2q) = 2$

$\Leftrightarrow 2(p^2 + p - 2q^2 - 2q) = 1$, ce qui est impossible donc y est pair.

Si d divise x et y , alors d divise 1.

$(3x + 4y)^2 - 2(2x + 3y)^2 = x^2 - 2y^2 = 1$.

$3^2 - 2 \times 2^2 = 1$ donc $(3; 2)$ est solution.

À la calculatrice, on construit deux suites pour trouver $(3\ 363, 2\ 378)$ couple solution.

85 1. $n^2 + 5n + 4 = (n + 1)(n + 4)$, et $n^2 + 3n + 2 = (n + 1)(n + 2)$

2. $3n^2 + 15n + 19 = 3(n^2 + 5n + 4) + 7$
 $= 3(n + 1)(n + 4) + 7$

donc si $n + 1$ divise $3n^2 + 15n + 19$, alors $n + 1$ divise 7 donc $n + 1 = 1$ et $n = 0$ ou $n + 1 = 7$ et $n = 6$

3. Si $n = 0$, 2 ne divise pas 19. Si $n = 6$, 56 ne divise pas 217, donc $n^2 + 3n + 2$ ne divise pas $3n^2 + 15n + 19$.

86 $a = 5q + 3$.

$q = 5q' + r$ avec $r \leq 4$ donc $a = 25q' + 5r + 3$.

$r' = 5r + 3 \leq 23 < 25$. $r' \in \{3, 8, 13, 18, 23\}$

87 a. $a = bq + r$, $0 \leq r < b$ donc

$b^2 < a < b(q + 1)$ donc $b < q + 1$ donc

$r < b \leq q$. Dans la division de a par q , le quotient est b et le reste est r .

b. Si $a < b^2$, $bq \leq a < b^2$ donc $q < b$.

Si $r < q$, le quotient est b et le reste est r .

Si $q < r < b$, $a = (b + 1)q + r - q$, le quotient est $b + 1$ et le reste est $r - q$.

88 $a = bq + r$, $0 \leq r < b$ donc $a + 28 = bq + r + 28 = (b + 7)q + r = bq + r + 7q$ donc $7q = 28$ et $q = 4$.

89 $a = bq + r$, $0 \leq r < b$ donc $-a = b(-q) - r = b(-q - 1) + b - r$, avec $0 \leq b - r < b$, donc $0 \leq r < b$.

$2a = b(2q) + 2r$, si $0 \leq 2r < b$ et

$2a = b(2q + 1) + 2r - b$ si $2r \geq b$.

$na = b(nq) + nr$ et $nr = bq' + r'$

$na = b(nq + q') + r'$.

90 Le 14 juillet 2012 est un samedi. 223 ans se sont écoulés dont 54 bissextiles (1800 et 1900 ne le sont pas.) Soit n le nombre de jours écoulés : on a $365 \equiv 1 [7]$ donc $n \equiv 223 + 54 [7]$ donc $n \equiv -3 [7]$ Le 14 juillet 1789 était un mardi.

91 On pose 1991 : année 0 et samedi : jour 0. On appelle u_n le numéro du jour du 5 octobre de l'année n . Les années bissextiles sont donc congrues à 1 modulo 4. Ainsi, $u_1 = 2$ si $n \equiv 0 [4]$, $u_{n+1} \equiv u_n + 2 [7]$, sinon, $u_{n+1} \equiv u_n + 1 [7]$.

On cherche n tel que $u_n \equiv 0 [7]$. Avec un tableur ou un programme, on trouve $n \in \{5, 11, 22, 28, 33, 39, 50, 56, 61, 67\}$ soit 1996, 2002, 2013, 2019, 2024, 2030, 2041, 2047, 2052 et 2058.

92 Raisonner comme dans l'exercice 91, en prenant n pour différence d'âge.

93 a. Soit n est pair, soit il est impair et $n + 1$ est pair. Le produit $n(n + 1)$ est donc toujours pair.

b. c. Si $n \equiv r[p]$ et $r < p$, $n + k \equiv r + k[p]$, alors $n + p - r \equiv 0[p]$.

L'un des p nombres consécutifs est divisible par p , donc leur produit est divisible par p .

94 On cherche a, b, c , tels que
 $142 = a5^3 + b5^2 + c5 + d =$
 $(a5^2 + b5 + c)5 + d = ((a5 + b)5 + c)5 + d$.
 Or $142 = 28 \times 5 + 2$ donc $d = 2$, et $28 = 5 \times 5 + 3$
 donc $c = 3$, $b = 0$ et $a = 1$.

95 $a \equiv b[n]$ équivaut à n divise $a - b$ équivaut à
 $a = b + nk$. Si $0 \leq b < n$, b est le reste. Si $b \geq n$,
 b n'est pas le reste.

$n \equiv p - 1[p]$ donc $n \equiv -1[p]$ donc $n^2 \equiv 1[p]$ et $1 < p$.

96 a. Si $a \equiv 0[n]$, alors par produit, $a \times b \equiv 0[n]$.

b. $4 \times 9 = 36 = 6 \times 6$ donc $4 \times 9 \equiv 0 [6]$.

c. Faux : voir **b**.

97 a. Tous les couples dont l'un des membres
 est 0, ainsi que (2, 3), (3, 2), (4, 3), (3, 4).

b. (1, 1) et (5, 5).

98 a. Seuls les couples dont l'un des membres
 est nul.

b. (1, 1), (2, 4), (3, 5), (4, 2), (5, 3), (6, 6).

99 $1\ 000 = 27 \times 37 + 1$ donc $10^3 \equiv 1 [37]$ et par
 puissance, $10^{3n} \equiv 1 [37]$.

$10^{10} = 10^{9+1}$, $10^{20} = 10^{18+2}$ et $100 \equiv 26 [37]$.

100 a. $\bar{r} = 2$, $\bar{q} = 2$, $\bar{b} = 1$, $\bar{a} = 1$, $\bar{b}\bar{q} + \bar{r} = 4 \neq 1$
 donc c'est faux.

b. Si $a = bq + r$, par compatibilité avec les opéra-
 tions, $a \equiv bq + r, [9]$ et $a \equiv \bar{a} [9]$...

c. Non. Contre-exemple : si $a = 479\ 777$, $\bar{a} = 4$
 et $937 \times 515 + 218 = 482\ 773 \neq a$.

101 1. Voir TP Tice 1 page 23.

2. a. $5^6 = 15\ 625$ donc $S = 19 = 18 + 1$ et
 $5^6 \equiv 1 [9]$.

b. $2012 \equiv 5 [9]$ et $2012 \equiv 2 [6]$ donc $A = 2012^{6k+2}$
 $A \equiv 5^2 (5^6)^k [9]$, donc $A \equiv 7 [9]$; $A \equiv 7 [9]$,
 $B \equiv C [9]$, $C \equiv D [9]$ donc $D \equiv 7 [9]$

3. a. $A < (10^4)^{2012}$.

Chaque chiffre de A est inférieur à 9 donc
 $B \leq 72432$.

4. Le premier chiffre de B est inférieur ou égal à
 7, les autres à 9 donc $C \leq 43$.

5. d. $D < 12$ (si $C = 39$)

6. D'après 2.b., $D = 9k + 7$ et $D < 12$ donc $D = 7$.

102 a. $55 \equiv -1 [7]$, $56 \equiv 0 [7]$, $57 \equiv 1 [7]$, donc
 $u_n \equiv (-1)^n + 1 [7]$.

$u_n \equiv 0 [7] \Leftrightarrow n$ impair.

b. Pour tout n , $55^n \equiv 5 [10]$, $56^n \equiv 6 [10]$,

$u_n \equiv 0 [7] \Leftrightarrow 57^n \equiv 9 [10] \Leftrightarrow 7^n \equiv 9 [10]$.

Or $7^4 \equiv 1 [10]$ donc $7^n \equiv 9 [10] \Leftrightarrow n = 4k + 2$.

103 a. $u_1 = 64$, $u_2 = 314$, $u_3 = 1\ 564$, $u_4 = 7\ 814$.
 Si n est pair, u_n est terminé par 14, sinon par 64.

b. $u_{n+1} \equiv u_n + 2 [4]$ donc $u_{n+2} \equiv u_{n+1} + 2 [4]$,
 $u_{n+2} \equiv u_n [4]$.

$u_{2k} \equiv u_0 [4]$ et $u_{2k+1} \equiv u_1 [4]$.

c. Par récurrence, $2u_0 = 28 = 5^2 + 3$ et si
 $2u_n = 5^{n+2} + 3$ alors

$2u_{n+1} = 5(2u_n) - 12 = 5^{n+1+2} + 15 - 12 = 5^{n+3} + 3$.

Pour $k \geq 2$, $5^k \equiv 25 [10]$ donc $2u_n \equiv 28 [100]$.

d. $2u_n = 100m + 28$, $u_n = 50m + 14$ donc
 $u_m \equiv 2m + 2 [4]$.

$u_{2k} \equiv 2 [4]$ donc $m = 2s$ et $u_{2k} = 100s + 14$.

$u_{2k+1} \equiv 0 [4]$ donc $m = 2s + 1$ et $u_{2k} = 100s + 64$.

e. d divise u_n donc d divise 14 et 64. Les diviseurs
 positifs de 14 sont 1, 2, 7, 14 et ceux de 64 sont
 des puissances de 2 donc $d = 1$ ou $d = 2$.

104 Par produit, si $u_n \equiv 0 [9]$, $u_n^2 \equiv 0 [9]$ alors
 $u_{n+1} \equiv 0 [9]$. Si $a \equiv 0 [9]$, $u_n \equiv 0 [9]$ pour tout n .

Si $a \equiv -1 [9]$, $u_1 \equiv 0 [9]$, $u_n \equiv 0 [9]$ pour tout n .

Si $a \equiv 6 [9]$, $u_1 \equiv 6 [9]$, $u_n \equiv 6 [9]$ pour tout n .

Si $a \equiv 3 [9]$, $u_1 \equiv 3 [9]$, $u_n \equiv 3 [9]$ pour tout n .

Si $a \equiv 2 [9]$, $u_1 \equiv 6 [9]$, $u_n \equiv 6 [9]$ pour tout $n \geq 1$.

Si $a \equiv 1 [9]$, $u_1 \equiv 2 [9]$, $u_n \equiv 6 [9]$ pour tout $n \geq 2$.

Si $a \equiv 4 [9]$, $u_1 \equiv 2 [9]$, $u_n \equiv 6 [9]$ pour tout $n \geq 2$.

Si $a \equiv 5 [9]$, $u_1 \equiv 3 [9]$, $u_n \equiv 3 [9]$ pour tout $n \geq 1$.

Si $a \equiv 7 [9]$, $u_1 \equiv 2 [9]$, $u_n \equiv 6 [9]$ pour tout $n \geq 2$.

105 A. 1. $1^2 + 3^2 + 5^2 = 35 = 36 - 1 = 9 \times 4 - 1$
 donc $1^2 + 3^2 + 5^2 \equiv 2^2 - 1 [2^2]$.

2.

r	0	1	2	3	4	5	6	7
R	0	1	4	1	0	1	4	1

Les congruences modulo 8 des sommes de trois
 carrés sont 0, 1, 2, 4, 5, 6 mais pas 7.

B. 1. $2^n - 1 \equiv 1 [2]$, et x pair $\Leftrightarrow x^2$ pair (ex 78)
 donc les nombres impairs sont en nombre impair
 (soit 1, soit 3).

2. a. $x^2 + y^2 + z^2 = 4q^2 + 4r^2 + 4s^2 + 4s + 1 =$
 $4(q^2 + r^2 + s^2 + 4s) + 1$

b. Si $n \geq 3$, alors $2^n - 1 \equiv -1 [4]$ donc $2^n - 1 \equiv 3 [4]$
 et $3 \neq 1$

3. a. Voir ex 93.a.

b. $x^2 + y^2 + z^2 = 4(q^2 + q) + 4(r^2 + r) + 4(s^2 + s)$
 $+ 3 \equiv 3 [8]$

c. Si $n \geq 3$, alors 8 divise 2^n donc si
 $x^2 + y^2 + z^2 \equiv 2^n - 1 [2^n]$, alors

$x^2 + y^2 + z^2 \equiv k2^n + 2^n - 1$ donc

$x^2 + y^2 + z^2 \equiv 7 [8]$.

Or $3 \neq 7$ donc la seule solution est fournie par 1.

106 a. Voir ex 98 : $3 \times 5 \equiv 1 [7]$.

b. Si $x \equiv 6 [7]$, par produit, $3x \equiv 18 [7]$ donc
 $3x \equiv 4 [7]$.

Si $3x \equiv 4 \pmod{7}$ alors $5 \times 3x \equiv 20 \pmod{7}$; or $5 \times 3 \equiv 1 \pmod{7}$ donc $5 \times 3 \times x \equiv x \pmod{7}$ et par transitivité, $x \equiv 6 \pmod{7}$.

107 1. $7 - 3 \times 2 = 1$; $1 + 3 \times 2^2 = 13$;
 $1 + 3 \times 2^3 = 25$; $1 + 3 \times 2^4 = 7^2$.

Donc $(1 ; 1)$ et $(2 ; 4)$ sont solutions.

2. a. $m \geq 5$ donc $3 \times 2^m \equiv 0 \pmod{32}$, donc $7^n \equiv 1 \pmod{32}$.

b. $7^4 \equiv 1 \pmod{32}$, $7^{4k+1} \equiv 7 \pmod{32}$, $7^{4k+2} \equiv 17 \pmod{32}$,
 $7^{4k+3} \equiv 23 \pmod{32}$, donc $7^n \equiv 1 \pmod{32} \Leftrightarrow n = 4k$.

3. $7^n \equiv 2^{4k} \pmod{5}$ et $2^4 \equiv 1 \pmod{5}$ alors $7^n \equiv 1 \pmod{5}$.

4. Or 5 ne divise pas 3×2^m quelque soit m ,
donc si $m \geq 5$, il n'y a pas de solution.

5. $(1 ; 1)$ et $(2 ; 4)$ sont les seuls couples solutions.

108 1. $S = \{-1/2 ; 4/3\}$ qui ne sont pas entières

2. a. $6 \equiv -1 \pmod{7}$ donc par somme,

$$P \equiv -n^2 - 5n - 4 \pmod{7}.$$

b. Si $2a \equiv 5 \pmod{7}$, alors $-n^2 - 5n - a^2 \equiv -(n+a)^2 \pmod{7}$
 $P \equiv (a^2 - 4) - (n+a)^2 \pmod{7}$.

c. $2 \times 6 \equiv 5 \pmod{7}$.

$$d. P \equiv -(n+6)^2 + 4 \pmod{7}.$$

e. On peut prendre $c = 2$ ou $c = 5$ pour $c^2 \equiv 4 \pmod{7}$.

f. $P \equiv (2 - n - 6)(2 + n + 6) \pmod{7}$ et

$$P \equiv 0 \pmod{7} \Leftrightarrow n \equiv -4 \pmod{7} \text{ ou } n \equiv -1 \pmod{7} \text{ (voir ex 98)}$$

g. Avec $c = 5$, $P \equiv (5 - n - 6)(5 + n + 6) \pmod{7}$ et
 $P \equiv 0 \pmod{7} \Leftrightarrow n \equiv -4 \pmod{7} \text{ ou } n \equiv -1 \pmod{7}$. Les solutions
sont les mêmes.

3. On calcule $6n^2 - 5n - 4$ modulo 7 pour $n \equiv r \pmod{7}$
et $r \in \{0, 1, 2, 3, 4, 5, 6\}$. $P \equiv 0 \pmod{7} \Leftrightarrow r = 3$ ou
 $r = 6$.

109 1. $6x + 7y + 8z \equiv y \pmod{2}$ et $57 \equiv 1 \pmod{2}$ donc
 $y \equiv 1 \pmod{2}$.

2. $6x + 7(2p + 1) + 8z \equiv -p - z + 1 \pmod{3}$ et $57 \equiv 0 \pmod{3}$
donc $p + z \equiv 1 \pmod{3}$ et $1 < 3$.

3. $z = 3q + 1 - p$ et en remplaçant dans (E),
 $6x + 6p + 2 + 4q = 42$ donc $x + p + 4q = 7$.

si $q \geq 2$, $x + p + 4q \geq 8$ donc $q < 2$.

4. $q = 1$ $x + p = 3$ donc $(0, 7, 1)$, $(1, 5, 2)$, $(2, 3, 3)$
et $(3, 1, 4)$ sont solutions.

si $q = 0$, $x + p = 7$ et $z = 1 - p$ $p = 1$ ou $p = 0$ donc
 $(6, 3, 0)$, $(7, 1, 1)$.

110 On considère l'équation (E) : $6x^2 - 5y^2 = 7$
dont les inconnues x et y sont des entiers relatifs.

1. $6 \equiv 1 \pmod{5}$ et $7 \equiv 2 \pmod{5}$ donc $x^2 \equiv 2 \pmod{5}$.

2. $a \equiv r \pmod{5}$, $r \leq 4$.

r	0	1	2	3	4
r^2	0	1	4	4	1

3. Aucun carré n'est congru à 2 modulo 5. Il n'y
a donc pas de solution.

111 a. $13 \equiv 1 \pmod{3}$ et $23 < -1 \pmod{3}$, donc
 $3u + 13v + 23w \equiv v - w \pmod{3}$.

b. $3u = -13(3k + r) - 23(3k' + r') =$
 $3(-13k - 23k' - 12)$.

c. Pour $r = 0$, $-2 \leq k \leq 2$ et $-2 \leq k' \leq 2$, seul
 $(0 ; 0 ; 0)$ convient comme solution.

Pour $r = 1$, $-3 \leq k \leq 2$ et $-3 \leq k' \leq 2$, les solu-
tions possibles sont $(-2 ; 4 ; -2)$ et $(1 ; -2 ; 1)$.

Pour $r = 2$, $-3 \leq k \leq 2$ et $-3 \leq k' \leq 2$, les solu-
tions possibles sont $(2 ; -4 ; -2)$ et $(-1 ; 2 ; -1)$.

112 Soit n un entier naturel et $A_n = 3^{2n} - 2^n$.

1. $A_0 = 0$, $A_1 = 7$, $A_2 = 77$, $A_3 = 721$, que divisent 7.

2. a. $A_{n+1} = 3^{2(n+1)} - 2^{n+1} = 9 \times 3^{2n} - 2 \times 2^n =$
 $9 \times (A_n + 2^n) - 2 \times 2^n$.

b. $A_{n+1} = 9 \times A_n + 2^n(9 - 2) = 9 \times A_n + 7 \times 2^n$.
7 divise A_0 et 7. Si 7 divise A_n , 7 divise A_{n+1} .

2. a. En développant, on obtient

$$(a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) = a^n - b^n.$$

b. $A_n = 9^n - 2^n = (9 - 2) \cdot Q_n = 7Q_n$ et $Q_n \in \mathbb{N}$.

3. $9 \equiv 2 \pmod{7}$ donc par élévation à la puissance,
 $9^n \equiv 2^n \pmod{7}$ et $A_n \equiv 0 \pmod{7}$.

b. 7 divise A_n pour tout n .

113 Posons $n = k + 1$ et $k \geq 0$, et

$$A_k = 3 \times 5^{2k+1} + 2^{3k+1}.$$

$$A_k = 15 \times 25^k + 2 \times 8^k \text{ donc}$$

$A_k \equiv 15 \times 8^k + 2 \times 8^k \pmod{17}$ donc $A_k \equiv 0 \pmod{17}$ et
17 divise A .

114 Tableau modulo 11 :

n	0	1	2	3	4	5	6	7	8	9	10
3^n	1	3	9	6	7	-1	-3	-9	-6	-7	1
A	5	9	10	4	6	1	-3	-4	-9	0	5

Si $n = 10k + r$, alors $3^n \equiv 3^r 3^{10} \pmod{11}$ donc $3^n \equiv 3^r \pmod{11}$
et 11 divise $2 \times 3^n + 3$ si et seulement si $n = 10k + 9$.

115 Si $n \equiv r \pmod{7}$, $N \equiv r^3 - 3r + 5 \pmod{7}$

r	0	1	2	3	4	5	6
r^2	0	1	4	2	2	4	1
r^3	0	1	1	-1	1	-1	-1
N	5	3	0	2	1	3	0

a. $N \equiv 0 \pmod{7} \Leftrightarrow n \equiv 2 \pmod{7}$ ou $n \equiv 6 \pmod{7}$

b. $N \equiv 1 \pmod{7} \Leftrightarrow n \equiv 4 \pmod{7}$.

116 1. $A = ab(a - b)(a + b)$.

Si 3 divise a ou b , alors 3 divise A .

Sinon, $a = 3k + 1$ ou $3k + 2$ et b aussi.

Si $a = 3k + 1$ et $b = 3k + 1$, alors 3 divise $a - b$.
 Si $a = 3k + 1$ et $b = 3k + 2$, alors 3 divise $a + b$.
 Même chose pour les deux autres cas.

2. a. Si $a \equiv 0 [3]$ alors $a^2 \equiv 0 [3]$.

Si $a \equiv 1 [3]$ alors $a^2 \equiv 1 [3]$

Si $a \equiv 2 [3]$ alors $a^2 \equiv 1 [3]$

b. Si $a \equiv 0 [3]$ ou $b \equiv 0 [3]$, alors $A \equiv 0 [3]$.

Sinon $a^2 - b^2 \equiv 0 [3]$ donc $A \equiv 0 [3]$.

117 a. $n = 100c + 10d + u$ donc $n \equiv 2d + u [4]$
 et $n \equiv 0 [4] \Leftrightarrow 2d + u \equiv 0 [4]$

b. $n \equiv -7c + 10d + u [107]$

Si $n \equiv 0 [107]$, $10d \equiv 7c - u [107]$ donc

$100d^2 \equiv (7c - u)^2 [107]$ et

$7d^2 + (7c - u)^2 \equiv 0 [107]$.

118 $u_0 = 0, u_1 = 0, u_2 = 27, u_3 = 54$.

$u_{n+1} + 2u_n = (3n + 2)^2 - 2 + (-2)^{n+1} + 2(3n - 1)^2 - 4 - (-2)^{n+1}$.

$u_{n+1} + 2u_n = 27n^2$ donc $u_{n+1} = -2u_n + 27n^2$.

27 divise u_0 et si 27 divise u_n , 27 divise u_{n+1} .

Par récurrence, pour tout n , 27 divise u_n .

119 $A = a \times 11^3 + b \times 11^2 + c \times 11 + a = b \times 7^3 + b \times 7^2 + a \times 7 + c$ donc $1\ 325a + 10c = 271b$.

$b \equiv 5a [10]$ donc $b = 5a + 10k$, avec $a \leq 6$ et $b \leq 6$ donc $a = 1$ et $b = 5$ ou $a = b = 0$ et $c = 0$ donc $N = 0$, ou $a = 1$ et $b = 5$ et $1\ 375 = 271b$ qui n'a pas de solution dans $\mathbb{N}$.

120 $N = x \times 6^2 + 3 \times 6 + y = 36x + y + 18 = 9k$ donc 9 divise y et $y \leq 6$ donc $y = 0$ et $N = 18(2x + 1)$.

$100 < 36x + 18 < 200$ donc $3 \leq x \leq 5$ et

$N \in \{132, 168, 198\}$

121 1. $72 = 1 \times 72 = 2 \times 36 = 3 \times 24 = 4 \times 18 = 6 \times 12 = 8 \times 9$

2. a. $P = p^2 - 6p + 9 - 72 = (p - 3)^2 - 72$.

b. $p^2 - 6p - 63 = q^2 \Leftrightarrow (p - 3)^2 - q^2 = 72$

$\Leftrightarrow (p - 3 - q)(p - 3 + q) = 72 \Leftrightarrow x = p - q - 3$ et

$y = p + q - 3$; $xy = 72 \Leftrightarrow xy = 72$, et $2p = x + y + 6$;
 $2q = y - x$.

$x + y$ doit être pair donc x et y ont même parité, et $x < y$ donc $(x, y) \in \{(2, 36), (4, 18), (6, 12)\}$ et $(p, q) \in \{(22, 17), (14, 7), (12, 3)\}$.

122

k	0	1	2	3	4	5	6
$5^k \bmod 7$	1	5	4	6	2	3	1

$5^{6k} \equiv 1 [7]$ et si $n = 6k + r$, alors $r \leq 5$, $5^n \equiv 5^r [7]$.

$5^{6n} + 5^n + 2 \equiv 0 [7] \Leftrightarrow 5^n \equiv 4 [7] \Leftrightarrow n = 6k + 2$.

123

k	0	1	2	3	4
$2^k \bmod 5$	1	2	4	3	1

$2^{4k} \equiv 1 [5]$ et si $n = 4k + r$, alors $r \leq 3$, $2^n \equiv 2^r [5]$.

$917541 \equiv 1 [4]$ donc $2^{917541} \equiv 2 [5]$.

124 Si $n = r [6]$, $N \equiv r(r + 1)(2r + 1) [6]$.

$N \equiv 0 [6]$, pour $0 \leq r \leq 6$, donc $N \equiv 0 [6]$.

125

k	0	1	2	3	4	5	6
$2^k \bmod 9$	1	2	4	8	7	5	1

$2^{6k} \equiv 1 [9]$ et si $n = 6k + r$, alors $r \leq 5$, $2^n \equiv 2^r [9]$.

a. $2^n \equiv 1 [9] \Leftrightarrow n = 6k$.

b. $11 \equiv 2 [9]$ donc $2^x 11^y \equiv 2^{x+y} [9]$ donc

$2^{x+y} \equiv 1 [9] \Leftrightarrow x + y = 6k$.

126 a. $6 \equiv -1 [7]$ donc $6^n \equiv (-1)^n [7]$.

k	1	2	3	4	5	6
$4^k \bmod 7$	4	2	1	4	2	1
$5^k \bmod 7$	5	4	6	2	3	1

b. $5^{6k} \equiv 1 [7]$ et si $n = 6k + r$, $r \leq 5$, $5^n \equiv 5^r [7]$.

$4^{3k} \equiv 1 [7]$ et si $n = 3k' + r'$, $r' \leq 2$, $4^n \equiv 4^{r'} [7]$.

Or $7 = 4 + 2 + 1 = 4 + 4 - 1 = 2 + 6 - 1$.

Si n est pair, r est pair et $n = 6k + 2 = 3k' + 2$ ou $n = 6k + 4 = 3k' + 1$.

Si n est impair, r est impair et il n'y a pas de solution.

De plus $105 < 6k + 2 < 6k + 4 < 125 \Leftrightarrow$

$103 < 6k < 121$ donc $18 \leq k \leq 20$.

$n \in \{110, 112, 116, 118, 122, 124\}$

127 $N = a \times 10^3 + b \times 10^2 + c \times 10 + a = 1\ 001a + 100b + 10c$.

$N \equiv 2b + 3c [7]$. $N \equiv 0 [7] \Leftrightarrow 2b + 3c \equiv 0 [7]$

$b \leq 9, c \leq 9$.

Une étude de tous les cas montre que

$(b, c) \in \{(2, 1), (4, 2), (6, 3), (8, 4), (1, 4), (2, 8), (9, 1), (5, 6), (7, 7), (4, 9), (9, 8)\}$.

Or on sait que $N \equiv 11a + b + 10c [99]$.

En étudiant tous les cas, seuls 1 981 et 8 218 conviennent.

128 a. $5^{4k} \equiv 1 [13]$ et si $n = 4k + r$, $r \leq 3$, alors $5^n \equiv 5^r [13]$.

b. $1\ 981 \equiv 5 [13]$ et $1\ 981 \equiv 1 [4]$ donc

$1\ 981^{1981} \equiv 5 [13]$.

c. $31 \equiv 5 [13]$ et $18 \equiv 5 [13]$ donc

$N \equiv 5^{4n+1} + 5^{4n-1} [13]$ donc $N \equiv 5 + 5^3 [13]$ et

$N \equiv 0 [13]$.

129 1. $8 = 7 + 1$ donc $2^3 \equiv 1 [7]$ et par puissance on a $2^{3n} \equiv 1 [7]$. Ainsi, par produit, $2^{3n+1} \equiv 2 [7]$, et $2^{3n+2} \equiv 4 [7]$.

2. $2^{3k} \equiv 1 [7]$ et si $n = 3k + r$, $r \leq 2$, alors $2^n \equiv 2^r [7]$.

3. a. $A_p \equiv 3 [7]$.

b. $A_p = 2^{3n+1} + 2^{3 \cdot 2n+2} + 2^{3p}$, donc $A_p \equiv 2 + 4 + 1 [7]$ et enfin $A_p \equiv 0 [7]$.

c. $A_p = 2^{3n+2} + 2^{3 \cdot (2n+1)+1} + 2^{3p}$, donc $A_p \equiv 4 + 2 + 1 [7]$ et $A_p \equiv 0 [7]$.

4. $a = 2^3 + 2^6 + 2^9 = A_3$ et $b = 2^4 + 2^8 + 2^{12} = A_3$. b est divisible par 7, a ne l'est pas.

130 Dans cet exercice le message à décoder en question 2. est NSKE OHOE FSPE.

1. NANO JOE MCHXE

2. VOUS ETES BONS

3. a. Si $3n + 2 \equiv m [26]$, alors par somme, $3n \equiv m - 2 [26]$.

b. $3 \times 9 \equiv 1 [26]$.

c. Par produit, $27n \equiv n [26]$ donc $27n \equiv 9(m - 2) [26]$.

d. Si $n \equiv 9(m - 2) [26]$, alors $3n \equiv 27(m - 2) [26]$, et $3n + 2 \equiv m [26]$ donc $g(m) = 9m - 18$.

131 Dans cet exercice, en question 2.a. on veut montrer que $3n_2 = 3p_2 - 6p_1$. En question 2.c. le message à décoder est MPYORQZL.

1. NO $\rightarrow (13, 14) \rightarrow (5, 24) \rightarrow FY$

MB $\rightarrow (12, 1) \rightarrow (15, 5) \rightarrow PF$

RE $\rightarrow (17, 4) \rightarrow (19, 16) \rightarrow TQ$

2. a. $11p_1 - 5p_2 = 11(3n_1 + 5n_2) - 5(6n_1 + 11n_2) = 3n_1$.

$3p_2 - 6p_1 = -6(3n_1 + 5n_2) + 3(6n_1 + 11n_2) = 3n_2$.

b. Voir exercice 130.

MP YO RQ ZL $\rightarrow$ TR ES BI EN

132 1. $0 \leq r \leq 96$ donc $1 \leq K \leq 97 < 100$.

$A = 100N + K$, par définition de A .

2. $N \equiv r [97]$ donc $N \equiv -K [97]$ et $N + K \equiv 0 [97]$.

3. a. $N = a_{12} \cdot 10^{12} + \dots + a_m \cdot 10^m + \dots + a_0$ et $N' = a_{12} \cdot 10^{12} + \dots + a'_m \cdot 10^m + \dots + a_0$.

$N - N' = (a_m - a'_m)10^m$ avec $-9 \leq a_m - a'_m \leq 9$.

b. On étudie toutes les valeurs de a et celles de m .

c. La clé de contrôle ne convient plus et l'erreur est alors détectée.

4. $N = a_{12} \cdot 10^{12} + \dots + a \cdot 10^{m+1} + b \cdot 10^m + \dots + a_0$ et $N' = a_{12} \cdot 10^{12} + \dots + b \cdot 10^{m+1} + a \cdot 10^m + \dots + a_0$

$N - N' = 9(a - b)10^m$ avec $-9 \leq a - b \leq 9$

En étudiant tous les cas, 97 ne divise pas $9r \cdot 10^m$ donc l'erreur est détectée.

133 $B = 300034040100000615123^{**}$

Ce nombre de 22 chiffres est trop grand pour les calculatrices. On peut donc le partager en 2.

$A = 3000340401$, $C = 615123$ et $B = A \cdot 10^{11} + C$.

$A \equiv 33 [97]$, $B \equiv 46 [97]$, $10^2 \equiv 3 [97]$, donc

$10^{11} \equiv 10 \cdot 3^5 [97]$, par conséquent $10^{11} \equiv 5 [97]$

et $B \equiv 33 \times 5 + 46 [97]$. Ainsi $B \equiv 17 [97]$ donc

$K = 80$.

134 $n = a_{15}a_{14} \dots a_1a_0$.

a	1	3	8	7	2	4	9	6	3	0	9	4	7	9	4
m	2	6	7	5	4	8	9	3	6	0	9	8	5	9	8

$M(n) = a_0 + m(a_1) + \dots + m(a_{15}) \equiv 8 [10]$ donc ce n'est pas un numéro de carte.

Si $x \leq 4$, $m(x) = 2x$ est pair et si $x \leq 5$, $m(x)$ est la somme de deux chiffres dont le premier impair et le deuxième pair donc $m(x)$ impair et pour tout y de $\{0, \dots, 9\}$, il existe un unique x de $\{0, \dots, 9\}$ tel que $m(x) = y$.

Si un seul chiffre est erroné, la différence sera comprise entre 1 et 9, $M(n)$ ne peut-être congrue à 0 modulo 10 donc l'erreur est détectée.

135 a. Soit n le nombre de 1. $n(A) = 5$ donc $m = 1$.

b. Si $n(A)$ pair, $m = 0$ et si $n(A)$ est impair, $m = 1$.

c. Changer un 1 en 0 revient à changer la parité de $n(A)$ donc changer m .

L'erreur n'est pas détectée si on fait un nombre pair d'erreurs.

Préparer le BAC

Exercices guidés

148 1. a. $N = (2 + 4 + 5) + 7(3 + 1 + 4) = 11 + 56 = 67 = 6 \times 10 + 7$.

b. $N = (9 + 3 + 5) + 7(2 + 4 + 1) = 17 + 49 = 66 = 6 \times 10 + 6$. La clé est 6.

c. $N = (1 + x + 7) + 7(1 + 2 + 7) = 8 + x + 70$. $N \equiv 8 + x [10]$ donc $N \equiv 4 [10]$ équivaut à $x \equiv 6 [10]$ donc $x = 6$.

d. $N = (1 + 4 + 7) + 7(3 + x + 5) = 12 + 7x + 56 = 68 + 7x$. $N \equiv 8 + 7x [10]$ donc $N \equiv 2 [10]$ équivaut à $7x \equiv 4 [10]$. Par une étude de tous les cas, on trouve $x = 2$.

2. a. $N_1 = (x_1 + x_3 + x_5) + 7(x_2 + x_4 + x_6)$, $N_2 = (x_1 + x_3 + x_5) + 7(x_2 + x_3 + x_6)$, donc $N_1 - N_2 = 7(x_4 - x_3)$.

b. Par une étude de tous les cas, si $a \neq 0$, $7a \equiv b \pmod{10}$ avec $b \neq 0$.

c. Or la clé n'est pas changée donc $N_1 - N_2 \equiv 0 \pmod{10}$ donc $x_4 - x_3 \equiv 0 \pmod{10}$.

Si $x_4 \neq x_3$ la clé de N_2 ne conviendra pas.

3. L'erreur n'est pas détectée dans le cas où $N_1 \equiv N_2 \pmod{10}$ donc si $x_3 + 7x_2 \equiv x_2 + 7x_3 \pmod{10}$, d'où $6x_2 \equiv 6x_3 \pmod{10}$.

Si $x_2 = 1$ et $x_3 = 6$, alors $6x_2 \equiv 6x_3 \pmod{10}$ et l'erreur n'est pas détectée.

149 1. $5x_0 - y_0 + 3 = 5 - 8 + 3 = 0$ donc $M_0 \in \Delta$, et si $M_n \in \Delta$, $5x_{n+1} - y_{n+1} + 3 = 5x_n - y_n + 3 = 0$ donc $M_{n+1} \in \Delta$.

$y_n = 5x_n + 3 = 0$ donc en remplaçant,

$x_{n+1} = 4x_n + 2$.

2. Par récurrence, $x_0 \in \mathbb{N}$ et si $x_n \in \mathbb{N}$, $4x_n + 2 \in \mathbb{N}$ donc $x_{n+1} \in \mathbb{N}$.

3. a. $5 \times 0 \equiv 0 \pmod{3}$; $5 \times 1 \equiv 2 \pmod{3}$; $5 \times 2 \equiv 1 \pmod{3}$, donc $5x \equiv 0 \pmod{3}$ si et seulement si $x \equiv 0 \pmod{3}$.

b. $y_n = 5x_n \pmod{3}$ donc x_n est divisible par 3 si et seulement si y_n est divisible par 3.

c. Si d divise y_n et x_n alors d divise 3 donc $d = 1$ ou $d = 3$.

x_n n'est pas divisible par 3, donc $d = 1$.

4. a. Par récurrence, avec $x_{n+1} = 4x_n + 2$:

$\frac{1}{3}(4^0 \times 5 - 2) = 1 = x_0$ et si $x_n = \frac{1}{3}(4^n \times 5 - 2)$,

alors $x_{n+1} = 4 \times \frac{1}{3}(4^n \times 5 - 2) + 2 =$

$\frac{1}{3}(4^{n+1} \times 5 - 8) + 2 = \frac{1}{3}(4^{n+1} \times 5 - 2)$. La propriété est vraie pour $n = 0$ et elle est héréditaire : elle est donc vraie pour tout $n \in \mathbb{N}$.

b. D'après 2., $4^n \times 5 - 2 = 3x_n$ et $x_n \in \mathbb{N}$.

c. On peut raisonner avec les congruences modulo 3 : $4 \equiv 1 \pmod{3}$ donc par puissance, $4^n \equiv 1 \pmod{3}$ et $5 \equiv 2 \pmod{3}$, donc par produit $5 \times 4^n \equiv 2 \pmod{3}$, donc 3 divise $4^n \times 5 - 2$.

On peut aussi procéder par récurrence.

QCM – Vrai ou faux

150 a. Vrai. $11 \equiv 4 \pmod{7}$ et $4^3 \equiv 1 \pmod{7}$ et $4^{2011} \equiv 4 \pmod{7}$.

b. Faux. Les carrés sont congrus à 0 ou 1 modulo 3 donc $x^2 + y^2 \equiv 0 \pmod{3}$ équivaut à $x^2 \equiv 0 \pmod{3}$ et $y^2 \equiv 0 \pmod{3}$.

c. Faux. $2\,009^{8002} \equiv 1 \pmod{16}$. En effet $2\,009^{8002} \equiv 9^{8002} \pmod{16}$ et $81 = 16 \times 5 + 1$ donc $9^2 \equiv 1 \pmod{16}$.

On ne peut répondre à cette question dans ce chapitre ; elle sera traitée dans le chapitre 2.

151 a. Vrai. Les carrés sont congrus à 0, 1, 2 et 4 modulo 7. Aucune des sommes ne fait 0 (modulo 7) sauf 0 + 0.

b. Faux. $9 + 3 + 3 = 15$ et 3 n'est pas congru à 1 modulo 5.

c. Faux. $N = 7 + 10a + 100b + 1\,000a = 7 + 100b + 1\,001a$.

Or $100 \equiv 1 \pmod{7}$ et $1\,001 \equiv 0 \pmod{7}$ donc $N \equiv a \pmod{7}$.

d. Faux. 2^{3n+1} n'est pas divisible par 5.

e. Vrai. $5 \equiv -2 \pmod{7}$ donc $5^{6n+1} + 2^{3n+1} \equiv -2 + 2 \pmod{7}$.

152 a. C. Seul $x \equiv 5 \pmod{6}$ est solution.

b. B. $4^4 \equiv 4 \pmod{17}$ et $2005 = 4 \times 551 + 1$.

c. C. $3x - 1 = 5y$.

d. C. par propriété des congruences.

e. C. après étude de tous les cas A et B sont faux : $a = 2$ pour A, $a = 7$ pour B.

Exercice

153 1. a. $2\,009 = 11 \times 182 + 7$.

b. $2^{10} = 1024 = 11 \times 93 + 1$ donc $2^{10} \equiv 1 \pmod{11}$.

c. $2009 = 200 \times 10 + 9$ donc $2^{2009} \equiv 2^9 \pmod{11}$ et $2^9 \equiv 6 \pmod{11}$.

$2^{2009} + 2\,009 \equiv 2 \pmod{11}$ et $2 < 11$ donc le reste est 2.

2. $A_n = 2^n + p$.

d_n divise A_n et A_{n+1} , et divise donc $A_{n+1} - A_n = 2^n$ donc d_n divise 2^n .

3. $A_n \equiv p \pmod{2}$ donc A_n et p ont la même parité.

4. d_n divise A_n donc si p est impair, A_n est impair et d_n aussi. Si d_n est pair, A_n et p sont pairs donc d_n et p ont la même parité.

d_n divise 2^n donc $d_n = 1$ ou $d_n = 2^k$.

$p = 2\,019$ est impair donc $d = 1$ et c'est leur seul diviseur commun.

154 1. $4^3 \equiv 1 \pmod{7}$ donc si $n = 3q + r$, alors $4^n = 4^{3q+r} = 4^r \cdot (4^3)^q$ donc $4^n \equiv 4^r \pmod{7}$.

Si $n = 3q$ le reste est 1, si $n = 3q + 1$ le reste est 4, si $n = 3q + 2$ le reste est 2.

2. a. $851 = 121 \times 7 + 4$ donc $851 \equiv 4 \pmod{7}$.

b. $A \equiv 4^{3n} + 4^{2n} + 4^n \pmod{7}$.

Si $n = 3q$, $4^n \equiv 1 \pmod{7}$ et $A \equiv 3 \pmod{7}$ donc le reste est 3.

Si $n = 3q + 1$, $4^n \equiv 4 \pmod{7}$, $4^{2n} \equiv 2 \pmod{7}$, $4^{3n} \equiv 1 \pmod{7}$ et $A \equiv 0 \pmod{7}$ donc le reste est 0.

Si $n = 3q + 2$, $4^n \equiv 2 \pmod{7}$, $4^{2n} \equiv 4 \pmod{7}$, $4^{3n} \equiv 1 \pmod{7}$ et $A \equiv 0 \pmod{7}$ donc le reste est 0.

3. $B \equiv 2 \times 1 + 1 \times 2 + 3 \times 1 + 2 \times 2 + 4 + 1 \pmod{7}$ donc $B \equiv 2 \pmod{7}$; $2 < 7$ donc le reste de B par 7 est 2.

155 1. De tels nombres semblent être des multiples de 11, mais pas tous.

2. a. $n^2 + 11 - (n - 11)(n + 11) = 132$.

b. Si $n + 11$ divise $n^2 + 11$, alors $n + 11$ divise $132 = 11 \times 12$ donc $n + 11 \in \{11; 12; 22; 33; 44; 66; 132\}$, soit $n \in \{0; 1; 11; 22; 33; 55; 121\}$. Réciproquement, ces nombres conviennent.

Pour aller plus loin

156 Il existe dix chiffres donc parmi 11 entiers distincts, deux au moins ont le même chiffre des unités.

157 1. $u_{k+1} = 1 + 10 + 10^2 + \dots + 10^k = 1 + 10(1 + 10 + 10^2 + \dots + 10^{k-1}) = 10u_k + 1$.

2. a. $1\ 111\ 111 = 13 \times 8\ 547$

b. Les multiples de 10 sont terminés par 0 donc 10 n'est pas un div' 1.

c. Les entiers dont aucun multiple n'est terminé par 1 ne sont pas des div' 1. Les nombres pairs, les multiples de 5 par exemple.

3. a. Dans la division par n , il y a $n - 1$ restes non nuls. Or si $1 \leq k \leq n$, on a n restes. Si aucun des r_k est nul, il existe deux entiers p et q tels que $r_p = r_q$.

b. $u_k \equiv r_k[n]$ donc par opération, si $r_p = r_q$, $r_{p+1} \equiv r_{q+1}[n]$ c'est-à-dire $r_{p+m} \equiv r_{q+m}[n]$ pour tout m . Il n'y aura donc aucun reste nul et n n'est pas un div' 1.

158 1. $a^{n+1} = a \cdot a^n$ donc par produit, $r_{n+1} \equiv a r_n[b]$.

2. a. Dans la division par b , il y a b restes. Si $n \geq b$, au moins deux restes sont égaux.

b. Si $r_p = r_q$, alors $r_{p+1} \equiv a r_p[b]$ et $r_{q+1} \equiv a r_q[b]$ donc $r_{p+1} = r_{q+1}$.

c. $r_m = r_{m+s}$, $r_{m+k} = r_{m+k+s}$ et pour tout n de $\mathbb{N}$, $r_n = r_{n+s}$.

3. $a^{mq+s} = (a^m)^q \cdot a^s$ donc $r_{mq+s} \equiv r_m^q \cdot r_s$. S'il existe m tel que $r_m = 1$, alors $r_{mq+s} = r_s$.

159 1. Soit N l'ensemble des entiers $k > 0$ tels que $a^k \equiv 1[n]$.

N est non vide puisqu'il contient m , donc s existe.

2. a. $m = sq + r$ donc $a^{sq+r} = (a^s)^q \cdot a^r$ donc $a^m \equiv a^r[n]$ donc $a^r \equiv 1[n]$.

Or $0 \leq r < s$ et s est le plus petit non nul donc $r = 0$.

b. $n - 1 \equiv -1[n]$ donc $(n - 1)^2 \equiv 1[n]$

3. a. Si $a = 7q + r$, alors $a \equiv r[7]$. Il suffit de montrer que pour tout a compris entre 1 et 6, $a^6 \equiv 1[7]$.

b. À l'aide d'un tableau :

n/a	1	2	3	4	5	6	A_n
1	1	2	3	4	5	6	21
2	1	4	2	2	4	1	14
3	1	1	6	1	6	6	21
4	1	2	4	4	2	1	14
5	1	4	5	2	3	6	21
6	1	1	1	1	1	1	6
s	1	3	6	3	6	2	

3. Si $n = 6q + r$, $a^n \equiv a^r[7]$. (voir exercice 158)

D'après le tableau, A_n est divisible par 7 sauf pour les multiples de 6.

160 En utilisant le tableau de l'exercice 159, on voit que 3 et 5 sont racines primitives modulo 7 et que 2 et 3 sont racines primitives modulo 5.

$1^n = 1$ pour n donc 1 n'est jamais racine primitive modulo p .

$(p - 1)^2 \equiv 1[p]$ donc $p - 1$ est racine primitive modulo p si $p - 1 = 2$, soit $p = 3$.

161 1. a. b. $N = 12 = 8 + 4 = 2^3 + 2^2 + 0 + 0$.

c. Les nombres écrits avec 4 chiffres en base 2 sont inférieurs à 2^4 . Il y en a 16, de 0 à 15.

2. Soit $N = \overline{abcd}^2$

10	0	1	2	3	4	5
2	0	1	10	11	100	101

10	5	6	7	8	9	10
2	101	110	111	1 000	1 001	1 010

10	11	12	13	14	15
2	1 011	1 100	1 101	1 110	1 111

Les nombres de E_1 ont une écriture binaire de 4 chiffres dont le premier est 1.

Pour ceux de E_2 le deuxième est 1, pour ceux de E_3 , le troisième est 1 et pour ceux de E_4 , le quatrième est 1. S'il est dans E_i , son ième chiffre est 1, sinon il vaut 0 donc $N = m_1 m_2 m_3 m_4$ en base 2.

3. a. Si B ne ment pas, $M = 1\ 100110$, $a = 0$, $b = 0$, $c = 0$ donc $k = 0$.

b. B ment à la question Q5. $M = 1\ 100\ 010$, $a = 1$, $b = 0$, $c = 1$ et $k = 5$.

c. $M = 00011100$ donc $a = 1$, $b = 0$, $c = 0$ et $k = 1$, B a menti à la question Q1. donc en base 2, $N = 1001 = 9$.

162 $N = a \times 10^3 + b \times 10^2 + c \times 10 + a = 1\,001a + 100b + 10c$.

$N \equiv 2b + 3c \pmod{7}$. $N \equiv 0 \pmod{7} \Leftrightarrow 2b + 3c \equiv 0 \pmod{7}$
 $b \leq 9, c \leq 9$.

Une étude de tous les cas montre que
 $(b, c) \in \{(2, 1), (4, 2), (6, 3), (8, 4), (1, 4), (2, 8), (9, 1), (5, 6), (7, 7), (4, 9), (9, 8)\}$.

Or on sait que $N \equiv 11a + b + 10c \pmod{99}$.

En étudiant tous les cas, seuls 1 981 et 8 218 conviennent.

163 a. $a^{ds} = (a^d)^s$ donc $a^n - 1 = a^{ds} - 1 = (a^d - 1)((a^d)^{s-1} + (a^d)^{s-2} + \dots + 1)$. Ainsi $(a^d - 1)$ divise $a^n - 1$. (P)

b. $a^d = a^d - 1 + 1$ donc $a^d \equiv 1[a^d - 1]$. Par puissance, $a^{ds} \equiv 1^s[a^d - 1]$ donc $a^n \equiv 1[a^d - 1]$.

164 Par le calcul, et en utilisant $n \equiv 0[n]$, on obtient $ax \equiv c[b]$ et $by \equiv c[a]$.

$3x + 6y = 3(x + 2y) = 7$ et 3 ne divise pas 7.

$3x + 6y = 15 \Leftrightarrow x + 2y = 5$ donc le couple $(3, 1)$ est solution.

165 Soit $E = \{1, 2, 3, 4, 5, 6\}$

a.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

b. Dans chaque ligne et chaque colonne figurent tous les éléments de E .

c. $1 \times 1 \equiv 1 \pmod{7}$, $2 \times 4 \equiv 1 \pmod{7}$, $3 \times 5 \equiv 1 \pmod{7}$,
 $6 \times 6 \equiv 1 \pmod{7}$, donc $6! \equiv -1 \pmod{7}$

$a \times 2a \times 3a \times 4a \times 5a \times 6a \equiv 1 \times 2 \times 3 \times 4 \times 5 \times 6 \pmod{7}$ donc $-a^6 \equiv -1 \pmod{7}$ donc $a^6 \equiv 1 \pmod{7}$.

166 Il n'y a que n entiers impairs entre 1 et $2n$.

Tous ces entiers s'écrivent $m = a \cdot 2^k$ avec a impair, $a \leq 2n$ et $k \geq 0$. Au moins deux entiers ont le même a donc il existe m et m' tels que $m = a \cdot 2^k$ et $m' = a \cdot 2^{k'}$, $k < k'$ donc $m' = m \cdot 2^{k'-k}$, ainsi m divise m' .

167 $A(n) = 2 \times 7^{2n+1} + 3^{n+2}$.

$A(0) = 2 \times 7 + 3^2 = 23$.

$A(n+1) = 98 \times 7^{2n+1} + 3 \times 3^{n+2}$

$A(n+1) \equiv 6 \times 7^{2k+1} + 3 \times 3^{k+2} \pmod{23}$ donc

$A(n+1) \equiv 3 A(n) \pmod{23}$ donc si 23 divise $A(n)$, 23 divise $A(n+1)$.

Par récurrence, pour tout n , 23 divise $A(n)$.

168 Pour $p = 4$, $N = A = 1\,379 = 7 \times 197$ donc 13 797, 137 977 et 137 991 sont divisibles par 7.
 $10 \equiv 3 \pmod{7}$, $10^2 \equiv 2 \pmod{7}$, $10^3 \equiv -1 \pmod{7}$, $10^4 \equiv -3 \pmod{7}$,
et $10^5 \equiv -2 \pmod{7}$, de plus $7 \equiv 0 \pmod{7}$ et $9 \equiv 2 \pmod{7}$.

Pour $p = 5$, $A \equiv -3a - b + 2c + 3d + e \pmod{7}$ donc

$A \equiv 3(d - a) + 2c + (e - b) \pmod{7}$

avec a, b, c, d, e éléments de $\{0, 1, 2, 3\}$.

Si $d = a, c = 2, e = 3, b = 0$ on a 17 913 et 179 137.

Si $e = b, c = 2, d = 1, a = 0$ on a 73 913 et 739 137.

Si $c = 1, d = 3, a = 2, e = 2, b = 0$ on a 97 139 et 971 397.

Pour $p = 6$, on a déjà traité le cas où il y a deux 7 et deux 1 ou 3 ou 9, deux 1 et deux 9, et trois 7. Il reste 5 cas : trois 1, trois 3, trois 9, deux 1 et deux 3, et deux 3 et deux 9.

$A \equiv -2a - 3b - c + 2d + 3e + f = 2(d - a) + 3(e - b) + f - c \pmod{7}$.

Si $e = b, d = 3, a = 1, f = 3, c = 0$ on a 197 393.

Si $e = b, d = 3, a = 0, f = 2, c = 1$ on a 711 319, 731 339 et 791 399.

Si $f = c, d = 2, a = 0, e = 2, b = 1$ on a 713 993.

169 On pose $A = \frac{n^3 + 1}{nm - 1}$.

Si $mn - 1$ divise $n^3 + 1$, alors $mn - 1$ divise $m^3n^3 + m^3 = (m^3 + 1) + (m^3n^3 - 1)$. Comme $mn - 1$ divise $(mn)^3 - 1$, cela implique que $mn - 1$ divise $m^3 + 1$. Le problème est donc symétrique en m et n et il suffit d'étudier les deux cas $m = n$ et $m > n$.

• Si $n = m$ alors $n^3 + 1 = (n + 1)(n^2 - n + 1)$ donc

$$A = \frac{n^3 + 1}{n^2 - 1} = \frac{n^2 - n + 1}{n - 1} = n + \frac{1}{n - 1}.$$

A n'est entier que si $n = 2$;

• Si $n^3 + 1 \equiv 1[n]$ alors $mn - 1 \equiv -1[n]$; si A est entier et $A \equiv a[n]$ alors $n^3 + 1 = A(mn - 1)$ donc $1 \equiv -a[n]$ et $a \equiv -1[n]$ donc $A = kn - 1$.

Si $n = 1$, $m - 1$ divise 2 ssi $m - 1 = 1$ ou $m - 1 = 2$. Les couples $(1, 2)$ et $(1, 3)$ conviennent.

Soit $n > 1$.

Si $m > n > 1$, $mn > n^2$ donc

$$kn - 1 < n + \frac{1}{n - 1}.$$

Ainsi $(k - 1)n < 1 + \frac{1}{n - 1} < 2$ donc $k = 1$.

Or $(nm - 1)(n - 1) = n^3 + 1$ donc

$$m = \frac{n^2 + 1}{n - 1} = n + 1 + \frac{2}{n - 1} \text{ donc } n = 2, m = 5 \text{ ou } n = 3, m = 5.$$

Finalement, on a neuf solutions : $(2, 2), (2, 1), (3, 1), (1, 2), (1, 3), (2, 5), (3, 5), (5, 2), (5, 3)$.

Communiquer à l'écrit ou à l'oral

Dans cet exercice il manque un chiffre dans le message codé : il s'agit de

259453285995406259494535905859

Message à décoder :

LES NOMBRES SONT PLEINS DE MYSTERES

Accompagnement personnalisé

AP1

A. 1. a divise b signifie qu'il existe un entier k tel que $b = ak$.

2. a divise b signifie qu'il existe un entier relatif tel que $b = ka$.

3. Faux car $\frac{7}{8}$ n'est pas un entier.

4. Pas d'équivalence car la réciproque est fautive.

5. Faux, 12 est multiple de 4 et de 6 mais pas de 24.

6. Si $a \equiv b[c]$, et $0 \leq b < c$ alors b est le reste dans la division euclidienne de a par c .

7. $a = 21 \times 23 + 22$ donc 22 est le reste dans la division de a par 23.

8. $27 \equiv 15 [12]$ donc $9 \equiv 5 [4]$, $27 = 12 + 15$ donc $9 = 4 + 5$.

9. Réciproque fautive. $10 \equiv 6 [4]$, mais $5 \equiv 3 [4]$ est faux.

10. Faux : $4 \times 9 \equiv 0 [6]$ mais $4 \equiv 0 [6]$ ou $9 \equiv 0 [6]$ est faux.

B. 1. Cette méthode n'aboutira à rien.

2. L'étude de tous les cas ne convient pas car l'ensemble à étudier est infini.

3. Pour résoudre $x^2 + 9y^2 = 100$, si (x, y) est solution, alors $y^2 \leq 11$ donc il n'y a qu'un nombre fini de cas à étudier.

4. On peut factoriser et trouver les diviseurs de 20 ou bien raisonner modulo 3.

AP3

1. Voir TP TICE1 page 23.

2. Si $a \equiv r[b]$, a est le reste dans la division par b équivalent à $0 \leq r < b$.

a. $25 = 21 + 4$, $5^2 \equiv 4 [7]$, donc par produit, $5^3 \equiv 4 \times 5 [7]$. Or $20 = 21 - 1$ donc $5^3 \equiv -1 [7]$, et par puissance, $5^6 \equiv 1 [7]$, donc $5^{6k} \equiv 1 [7]$.

b. Si $n = 6k + r$, $r \leq 5$, alors $5^n = 5^{6k+r} = 5^{6k} \cdot 5^r = 5^n \equiv 5^{6k} \cdot 5^r [7]$ et $5^{6k} \equiv 1 [7]$, donc $5^{6k} \cdot 5^r \equiv 5^r [7]$.

c. $2\,014 = 335 \times 6 + 4$ donc $5^{2014} \equiv 5^4 [7]$, et $5^4 \equiv 2 [7]$ avec $2 < 7$ donc le reste est 2.

3.

r	0	1	2	3	4	5	6	7	8	9	10
r^2	0	1	4	9	5	3	3	5	9	4	1
r^4	0	1	5	4	3	9	9	3	4	5	1
r^5	0	1	-1	1	1	1	-1	-1	-1	1	1

Pour tout x , x^5 est congru à 0, 1 ou -1 modulo 11 donc $x^5 - 4$ est congru à -4, -3 ou -5 soit à 7, 6 ou 8. Or aucun carré n'est congru à 6, 7, ou 8 modulo 11. L'équation n'a donc pas de solution dans $\mathbb{N}$.

4.

r	-3	-2	-1	0	1	2	3
r^2	2	4	1	0	1	4	2

La seule somme de deux carrés nulle modulo 7 est $0 + 0 = 0$.

Exemple :

$(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1)$. Si k est pair, $k(k + 1)$ est pair.

Si k est impair, $k + 1$ est pair. $k(k + 1) = 2p$ donc $n^2 = 8p + 1$.

AP4

La cryptographie

Blaise de Vigenère (1523–1596) est un diplomate, écrivain et traducteur qui, en poste à Rome, se passionna pour la cryptographie et étudia les idées d'Alberti. Son nom resta car c'est lui qui inventa le « carré de Vigenère ».

Le chiffre de Vigenère est un chiffrement poly-alphabétique : une lettre peut être codée par plusieurs lettres différentes.

Principe du chiffre de Vigenère

– On écrit le texte à coder.

– On écrit en dessous le mot-clé en le répétant autant que nécessaire.

– À chaque lettre à coder on associe son rang n et le rang c de la lettre de la clé, la lettre codée a pour rang le reste de $n + c$ dans la division euclidienne par 26.

Le carré de Vigenère

Pour faciliter le codage et le décodage sans trop de calculs, Vigenère imagina le tableau connu sous le nom du « carré de Vigenère » (il contient l'alphabet en clair suivi de 26 alphabets codés, chacun étant déduit du précédent par décalage d'une lettre).

Début du carré de Vigenère :

Clair	A	B	C	D	E	F	G	H	I	J	K	L
Clé	0	1	2	3	4	5	6	7	8	9	10	11
A	0	A	B	C	D	E	F	G	H	I	J	K
B	1	B	C	D	E	F	G	H	I	J	K	L
C	2	C	D	E	F	G	H	I	J	K	L	M
D	3	D	E	F	G	H	I	J	K	L	M	N
E	4	E	F	G	H	I	J	K	L	M	N	O
F	5	F	G	H	I	J	K	L	M	N	O	P
G	6	G	H	I	J	K	L	M	N	O	P	Q
H	7	H	I	J	K	L	M	N	O	P	Q	R
I	8	I	J	K	L	M	N	O	P	Q	R	S
J	9	J	K	L	M	N	O	P	Q	R	S	T
K	10	K	L	M	N	O	P	Q	R	S	T	U
L	11	L	M	N	O	P	Q	R	S	T	U	V

Exemple

Clair	A	L	B	E	R	T	I
n	0	11	1	4	17	19	8
Clé	c	o	d	e	c	o	d
C	2	14	3	4	2	14	3
$(n + c) \bmod 26$	2	25	4	8	19	7	11
Code	C	Z	E	I	T	H	L

Pour la lettre B de ALBERTI : $n = 1$ et $c = 3$ (correspondant à la lettre D), d'où $n + c = 4$, donc le code associé est E (qui se trouve dans le carré de Vigenère à l'intersection de la colonne de B et de la ligne de D).

Pour la lettre T de ALBERTI : $n = 19$ et $c = 14$, d'où $n + c = 33$ et $33 \equiv 7 [26]$, le code est H.

Pour décoder, au lieu d'ajouter c on retranche c (le destinataire connaît la clé). En utilisant le carré de Vigenère, pour décoder le E trouvé ci-dessus, on repère sur la ligne 3 (correspondant au D de la clé) la place de E, et on lit la lettre en haut de la colonne, soit B.

Longtemps ce code fut indéchiffrable. Évidemment plus la clé est longue (une poésie, ou une citation d'un livre), plus il est difficile à déchiffrer. Il fut finalement cassé vers 1850.

Les cryptographes comprirent qu'il était nécessaire de changer très souvent de clé et d'utiliser une clé qui n'a aucun sens et si possible générée de manière aléatoire, ce qui fut réalisé avec la machine ENIGMA (1920).