ARITHMÉTIQUE

2

PGCD et PPCM. Théorèmes de Bézout et Gauss

Connaissances nécessaires à ce chapitre

- Déterminer le pgcd de deux entiers
- Savoir reconnaître deux nombres premiers entre eux
- Déterminer le ppcm de deux entiers
- Connaître le langage des congruences
- Trouver une solution évidente entière à une équation du type $ax + by = c$

Auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

1 « pgcd » signifie plus grand commun diviseur.

1) Calculer le pgcd de 26 et 65, puis simplifier $\frac{26}{65}$.

2) Calculer le pgcd de 72 et 54, puis simplifier $\frac{72}{54}$.

3) Calculer le pgcd de 255 et 35, puis simplifier $\frac{255}{35}$.

2 Deux nombres sont premiers entre eux s'ils ont un pgcd égal à 1.

9 et 16 sont-ils premiers entre eux ? 25 et 36 ?

3 « ppcm » signifie plus petit commun multiple.

1) Calculer le ppcm de 8 et 12, puis simplifier $\frac{15}{8} - \frac{13}{12}$.

2) Calculer le ppcm de 6 et 15, puis simplifier $\frac{5}{6} + \frac{4}{15}$.

3) Calculer le ppcm de 35 et 7, puis simplifier $\frac{3}{35} - \frac{3}{7}$.

4) Calculer le ppcm de 3 et 8, puis simplifier $\frac{7}{3} + \frac{3}{8}$.

4

1) Quelle relation y-a-t-il entre le pgcd et le ppcm de deux nombres ?

2) Soit $\text{pgcd}(a, b) = 8$ et $ab = 240$, calculer $\text{ppcm}(a, b)$.

5 Les phrases suivantes sont-elles vraies ou fausses ? Justifier.

1) Un nombre a est divisible par 6 et 9, donc a est divisible par 54.

2) Un nombre a est divisible par 8 et 9, donc a est divisible par 72.

3) Un nombre a est divisible par 4 et 18, donc $a \equiv 36\ (36)$.

4) Un nombre a est divisible par 10 et 15 donc $a \equiv 0\ (150)$.

6 Les phrases suivantes sont-elles vraies ou fausses. Justifier.

1) Si $x \equiv 0\ (81)$, alors $x \equiv 0\ (9)$.

2) L'équation $x^2 + 2y^2 \equiv 3\ (4)$ admet des solutions.

7 Trouver un couple d'entiers évident vérifiant les équations suivantes :

1) $7x - 10y = 1$

2) $4x + 5y = 1$

3) $3x + 4y = 3$

Voir solutions p. ??

ACTIVITÉ 1 Un algorithme célèbre

On donne l'algorithme suivant ci-contre où E() signifie la partie entière du nombre entre parenthèses.

1) On saisit $a = 391$ et $b = 221$.

a) Remplir ce tableau, en calculant à la main les différentes boucles du programme :

	a	b	q	r
Étape 0	391	221	1	170
Étape 1				
Étape 2				
Étape 3				

b) Quelle valeur affiche l'algorithme ?

```
1.  Liste des variables utilisées
2.    a, b, q, r : entiers
3.  Entrées
4.    Saisir a, b
5.    Donner à q la valeur de E(a/b)
6.    Donner à r la valeur de a − bq
7.  Traitements
8.    Tant que (r ≠ 0) faire
9.      Donner à a la valeur de b
10.     Donner à b la valeur de r
11.     Donner à q la valeur de E(a/b)
12.     Donner à r la valeur de a − bq
13.   Fin Tant que
14. Affichage
15.   Afficher la valeur b
```

3) Rentrer cet algorithme dans votre calculatrice, puis tester votre programme en complétant le tableau suivant :

a	12	18	30	24	60	150
b	8	12	5	18	84	240
Résultat						

4) Cet algorithme s'appelle l'algorithme d'Euclide. Il procède par divisions successives. Que calcule-t-il ?

ACTIVITÉ 2 Algorithme pour une solution particulière

Le but de cette activité est de déterminer un algorithme permettant de déterminer un couple d'entiers relatifs (x_0, y_0) solution de l'équation (E) : $59x + 27y = 1$

On suppose que cette équation admet des solutions entières.

1) Pourquoi peut-on trouver un entier naturel $x_0 > 0$ tel que le couple (x_0, y_0) soit solution de (E) ?

2) On s'intéresse à la quantité $59u + 27v$ où u et v varient sur $\mathbb{Z}$. On propose l'algorithme suivant pour calculer les valeurs de x_0 et y_0. E() signifie la partie entière du nombre entre parenthèses.

a) Que fait-on à la ligne 8 ?

b) Que calcule t-on à la ligne 9 ?

c) Expliquer la condition $(r \neq 1)$ dans la boucle conditionnelle.

d) Déterminer la valeur à donner à la variable v à la ligne 10, pour que v donne la valeur y_0.

e) Rentrer le programme dans votre calculatrice et donner une solution (x_0, y_0) de (E).

```
1.  Liste des variables utilisées
2.      u, v, r : entiers
3.  Entrées
4.      Donner à r la valeur de 0
5.      Donner à u la valeur de 0
6.  Traitements
7.      Tant que (r ≠ 1) faire
8.          Donner à u la valeur de u + 1
9.          Donner à r la valeur de 59u − 27 × E(59u/27)
10.     Fin Tant que
11.     Donner à v la valeur de ...
12. Affichage
13.     Afficher u, v
```

ACTIVITÉ 3 Chiffrement affine

Partie A : Un premier exemple

Afin de coder un message, on assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

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

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

Le chiffrement ou cryptage consiste à coder un message. Le déchiffrement consiste à décoder un message codé.

Un chiffrement élémentaire est le chiffrage affine. On se donne une fonction de codage affine f, par exemple : $f(x) = 11x + 8$.

À une lettre du message :

- on associe un entier x entre 0 et 25 suivant le tableau ci-dessus ;
- on calcule $f(x) = 11x + 8$ et l'on détermine le reste y de la division de $f(x)$ par 26 ;
- on traduit y par une lettre d'après le tableau ci-dessus.

Exemple : Si l'on veut coder par exemple la lettre G par la fonction $f(x) = 11x + 8$, on passe par les étapes suivantes :

$$\text{G} \Rightarrow x = 6 \Rightarrow 11 \times 6 + 8 = 74 \Rightarrow 74 \equiv 22\ (26) \Rightarrow y = 22 \Rightarrow \text{W}$$

La lettre G est donc codée par la lettre W.

1) Coder la lettre W.

2) Existence d'une fonction de décodage.

Théorème de Bézout : a et b sont deux entiers naturels. « a et b sont premiers entre eux » équivaut à « il existe deux entiers relatifs u et v tels que $au + bv = 1$ ».

a) Pourquoi le théorème de Bézout permet-il d'affirmer qu'il existe un entier relatif u tel que : $11u + 26v = 1$?

b) Montrer alors que l'équation $11x \equiv 1\ (26)$ puis que l'équation $11x \equiv j\ (26)$, j étant un entier naturel, admettent une solution.

3) Déterminer la fonction de décodage.

a) Montrer que pour tous entiers relatifs x et j, on a : $11x \equiv j\ (26) \quad \Leftrightarrow \quad x \equiv 19j\ (26)$.

b) En déduire que la fonction f^{-1} de décodage est $f^{-1}(y) = 19y + 4$ (modulo 26).

c) Décoder la lettre L.

Partie B : Codage et décodage

La fonction de codage est définie par la fonction f telle que : $f(x) = 21x + 11$

1) Coder le mot : ENIGME.
On pourra éventuellement remplir le tableau ci-contre.

Lettre	E	N	I	G	M	E
x	4					
$f(x)$	95					
y	17					
Code	R					

2) On cherche la fonction de déchiffrage f^{-1}.

a) Démontrer que pour tous relatifs x et z, on a : $21x \equiv z\ (26) \quad \Leftrightarrow \quad x \equiv 5z\ (26)$.

b) En déduire que la fonction de décodage est : $f^{-1}(y) = 5y + 23$.

c) Décoder le message RPERNL.
On pourra éventuellement remplir le tableau ci-contre.

Code	R	P	E	R	N	L
y	17					
$f^{-1}(y)$	108					
x						
Lettre						

Partie C : Casser une fonction de cryptage

On a reçu le message suivant : FMEYSEPGCB.

Par une étude statistique de la fréquence d'apparition des lettres sur un passage plus important, on déduit que le chiffrement est affine, que la lettre E est codée par la lettre E et que la lettre J est codée par la lettre N.

Soit la fonction affine f définie par : $f(x) = ax + b$ où a et b sont des entiers naturels compris entre 0 et 25.

1) Démontrer que a et b vérifient le système suivant : $\begin{cases} 4a + b \equiv 4\ (26) \\ 9a + b \equiv 13\ (26) \end{cases}$

2) a) Démontrer que $5a \equiv 9\ (26)$, puis que $a \equiv 7\ (26)$.

b) En déduire que $b \equiv 2\ (26)$ et que f est définie par $f(x) = 7x + 2$.

c) Démontrer que, pour tous relatifs x et z, on a : $7x \equiv z\ (26) \quad \Leftrightarrow \quad x \equiv 15z\ (26)$.

d) En déduire que la fonction de décodage f^{-1} est $f^{-1}(y) = 15x + 22$.

e) Décoder le message.

1. Plus grand commun diviseur

A. Définition et propriétés

DÉFINITION

Soit a et b deux entiers relatifs non tous nuls.
L'ensemble des diviseurs communs à a et b admet un plus grand élément d, appelé **plus grand commun diviseur**.

On note : $d = \text{pgcd}(a,b)$.

PREUVE *Existence*

L'ensemble des diviseurs communs à a et b est un ensemble fini car c'est l'intersection de deux ensembles finis.
De plus 1 divise a et b donc l'ensemble des diviseurs communs à a et b est non vide.
Or tout ensemble fini non vide dans $\mathbb{Z}$ admet un plus petit élément donc d existe.

Exemple $\text{pgcd}(24,18) = 6$, $\text{pgcd}(60,84) = 12$, $\text{pgcd}(150,240) = 30$

PROPRIÉTÉ

- $\text{pgcd}(a,b) = \text{pgcd}(b,a)$
- $\text{pgcd}(a,b) = \text{pgcd}(|a|,|b|)$
- $\text{pgcd}(a,0) = a$ car 0 est multiple de tout entier.
- Si b divise a, alors $\text{pgcd}(a,b) = |b|$.
- Pour tout entier naturel k non nul, on a : $\text{pgcd}(ka,kb) = k\,\text{pgcd}(a,b)$.

Exemple

- $\text{pgcd}(82,0) = 82$
- $\text{pgcd}(-24,-18) = \text{pgcd}(24,18) = 6$
- $\text{pgcd}(30,5) = 5$ car 30 est un multiple de 5.
- $\text{pgcd}(240,180) = 10\text{pgcd}(24,18) = 60$

B. Nombres premiers entre eux

DÉFINITION

On dit que a et b sont premiers entre eux si, et seulement si $\text{pgcd}(a,b) = 1$.

Exemple

- $\text{pgcd}(15,8) = 1$ donc 15 et 8 sont premiers entre eux.
- $\text{pgcd}(a,1) = 1$ donc 1 est premier avec tout entier.

ATTENTION : Il ne faut pas confondre des nombres premiers entre eux et des nombres premiers. 15 et 8 ne sont pas premiers et pourtant ils sont premiers entre eux.
Par contre, deux nombres premiers distincts sont nécessairement premiers entre eux.

C. Algorithme d'Euclide

THÉORÈME

Soit a et b deux naturels non nuls tels que b ne divise pas a.
La suite des divisions euclidiennes suivantes finit par s'arrêter. Le dernier reste non nul est alors le pgcd de a et de b.

$$\begin{array}{rll} a \text{ par } b & a = b\,q_0 + r_0 & \text{avec} \quad b > r_0 \geqslant 0 \\ b \text{ par } r_0 & b = r_0\,q_1 + r_1 & \text{avec} \quad r_0 > r_1 \geqslant 0 \\ r_0 \text{ par } r_1 & r_0 = r_1\,q_2 + r_2 & \text{avec} \quad r_1 > r_2 \geqslant 0 \\ \vdots & \vdots & \\ r_{n-2} \text{ par } r_{n-1} & r_{n-2} = r_{n-1}\,q_n + r_n & \text{avec} \quad r_{n-1} > r_n \geqslant 0 \\ r_{n-1} \text{ par } r_n & r_{n-1} = r_n\,q_{n-1} + 0 & \end{array}$$

On a alors $\text{pgcd}(a,b) = r_n$.

PREUVE

- La suite des restes : $r_0, r_1, r_2, \ldots, r_n$ est une suite strictement décroissante dans $\mathbb{N}$ car : $r_0 > r_1 > r_2 > \cdots > r_n$.
  D'après le principe de descente infinie, il existe alors n tel que $r_{n+1} = 0$.

  Montrons que $\text{pgcd}(a,b) = \text{pgcd}(b,r_0)$.

  Soit $D = \text{pgcd}(a,b)$ et $d = \text{pgcd}(b,r_0)$.

  D divise a et b donc D divise $a - bq_0 = r_0$, donc D divise b et r_0. Par conséquent $D \leqslant d$.
  d divise b et r_0 donc d divise $bq_0 + r_0 = a$, donc d divise a et b. Par conséquent $d \leqslant D$.

  On déduit de ces deux inégalités que $D = d$ d'où $\text{pgcd}(a,b) = \text{pgcd}(b,r_0)$.
- De proche en proche, on en déduit que :

$$\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = \cdots = \text{pgcd}(r_{n-2},r_{n-1}) = \text{pgcd}(r_{n-1},r_n)$$

  Or r_n divise r_{n-1}, donc $\text{pgcd}(r_{n-1},r_n) = r_n$
- Conclusion : $\text{pgcd}(a,b) = r_n$. Le dernier reste non nul est le pgcd.

MÉTHODE 1 Calculer le pgcd de deux nombres

► Ex. 13 p. 12

Exercice d'application Calculer $\text{pgcd}(4\,539, 1\,958)$.

Correction On effectue les divisions euclidiennes suivantes :

$$4\,539 = 1\,958 \times 2 + 623$$
$$1\,958 = 623 \times 3 + 89$$
$$623 = 89 \times 7$$

Conclusion : $\text{pgcd}(4\,539, 1\,958) = 89$

REMARQUE : Le petit nombre d'étapes montre la performance de cet algorithme.
ALGO On peut reprendre le programme de l'activité 1 pour automatiser l'algorithme d'Euclide.

2. Plus petit commun multiple

DÉFINITION

Soit a et b deux entiers relatifs non nuls.
L'ensemble des multiples strictement positifs communs à a et à b admet un plus petit élément m, appelé **plus petit commun multiple**.

On le note : $m = \text{ppcm}(a, b)$.

PREUVE *Existence*

L'ensemble des multiples strictement positifs à a et à b n'est pas vide. En effet $|ab|$ est un multiple positif de a et de b.
D'après le principe du bon ordre, cet ensemble admet un plus petit élément donc m existe.

Exemple

- $\text{ppcm}(18, 12) = 36$, $\text{ppcm}(24, 40) = 120$
- Pour additionner deux fractions, on recherche le dénominateur commun le plus petit qui n'est autre que le ppcm.

PROPRIÉTÉ

- Si b divise a, alors $\text{ppcm}(a, b) = |a|$.
- Si a et b sont premiers entre eux, alors $\text{ppcm}(a, b) = |ab|$.
- On a : $ab = \text{ppcm}(a, b) \times \text{pgcd}(a, b)$.

3. Théorème de Bézout

A. Égalité de Bézout

PROPRIÉTÉ

Soit a et b deux entiers non nuls et $D = \text{pgcd}(a, b)$.
Il existe alors un couple (u, v) d'entiers relatifs telle que : $au + bv = D$.

PREUVE

Soit G l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs.
G est une partie de $\mathbb{N}$ non vide : on vérifie facilement que $|a| \in G$.

D'après le principe du bon ordre, G admet donc un plus petit élément d tel que $d = au + bv$

- $D = \text{pgcd}(a, b)$ divise a et b donc D divise $au + bv = d$ et donc $D \leqslant d$.
- Montrons que d divise a.
  Divisons a par d, on a alors $a = dq + r$ avec $0 \leqslant r < d$.
  On isole le reste et on remplace d par $au + bv$:
  $$r = a - dq = a - auq - bvq = a(1 - uq) + b(-vq)$$
  Si $r \neq 0$ alors $r \in G$, or $r < d$ et d est le plus petit élément de G, cela est contradictoire.
  Donc $r = 0$ par conséquent d divise a.

PREUVE En faisant le même raisonnement, on montre que d divise aussi b.

d divise a et b, donc $d \leqslant D$.

- Conclusion : $D \leqslant d$ et $d \leqslant D$ donc $D = d$.

CONSÉQUENCE : : Tout diviseur commun à a et b divise leur pgcd.

B. Théorème de Bézout

THÉORÈME

Deux entiers relatifs a et b sont premiers entre eux **si et seulement si**, il existe deux entiers relatifs u et v tels que :

$$au + bv = 1$$

REMARQUE : La preuve du théorème de Bézout fait l'objet de l'exercice 24 p 13.

MÉTHODE 2 Montrer que deux nombres sont premiers entre eux

► Ex. 29 p. 13

Exercice d'application

Montrer que $(2n+1)$ et $(3n+2)$ sont premiers entre eux $n \in \mathbb{N}$.

Correction Il s'agit de trouver des coefficients u et v pour que $u(2n+1) + v(3n+2) = 1$.

$$-3(2n+1) + 2(3n+2) = -6n - 3 + 6n + 4 = 1$$

$\forall n \in \mathbb{N}$, il existe $u = -3$ et $v = 2$ tel que $u(2n+1) + v(3n+2) = 1$.

Les entiers $(2n+1)$ et $(3n+2)$ sont premiers entre eux.

MÉTHODE 3 Déterminer un couple (*u*,*v*) tel que *au* + *bv* = 1

► Ex. 35 p. 13

Exercice d'application

Montrer que 59 et 27 sont premiers entre eux puis déterminer un couple d'entiers relatifs (x, y) tel que : $59x + 27y = 1$.

Correction Pour montrer que 59 et 27 sont premiers entre eux, on effectue l'algorithme d'Euclide et pour déterminer un couple (x, y), on remonte celui-ci :

$$59 = 27 \times 2 + 5 \quad (1)$$
$$27 = 5 \times 5 + 2 \quad (2)$$
$$5 = 2 \times 2 + 1 \quad (3)$$

Le dernier reste est 1. Donc $\text{pgcd}(59, 27) = 1$ et 59 et 27 sont premiers entre eux.

On remonte l'algorithme d'Euclide : de (3)

$$2 \times 2 = 5 - 1$$

On multiplie l'égalité (2) par 2

$$27 \times 2 = 5 \times 10 + 2 \times 2$$

$$27 \times 2 = 5 \times 10 + 5 - 1$$
$$27 \times 2 = 5 \times 11 - 1$$
$$5 \times 11 = 27 \times 2 + 1$$

On multiplie l'égalité (1) par 11

$$59 \times 11 = 27 \times 22 + 5 \times 11$$
$$59 \times 11 = 27 \times 22 + 27 \times 2 + 1$$
$$59 \times 11 = 27 \times 24 + 1$$

On a donc :

$$59 \times 11 + 27 \times (-24) = 1$$

C. Corollaire de Bézout

PROPRIÉTÉ

L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple du pgcd(a, b).

Exemple

- L'équation $4x + 9y = 2$ admet des solutions car pgcd$(4, 9) = 1$ et 2 est multiple de 1.
- L'équation $9x - 15y = 2$ n'admet pas de solution car pgcd$(9, 15) = 3$ et 2 n'est pas multiple de 3.

4. Le théorème de Gauss

A. Le théorème

THÉORÈME

Soit a, b et c trois entiers relatifs non nuls.
Si a divise le produit bc et si a et b sont premiers entre eux alors a divise c.

PREUVE Si a divise le produit bc, alors il existe un entier k tel que : $bc = ka$.

Si a et b sont premiers entre eux, d'après le théorème de Bézout, il existe deux entiers u et v tels que : $au + bv = 1$.

En multipliant par c, on a :

$$acu + bcv = c \qquad \text{or } bc = ka, \text{ donc :}$$
$$acu + kav = c$$
$$a(cu + kv) = c$$

Donc a divise c.

Exemple Pour trouver les solutions dans $\mathbb{Z}^2$ de l'équation $5(x - 1) = 7y$, on sait que :

5 divise $7y$, or pgcd$(5, 7) = 1$, donc d'après le théorème de Gauss 5 divise y. On a donc : $y = 5k$

En remplaçant dans l'équation, on a :

$$5(x - 1) = 7 \times 5k \quad \Leftrightarrow \quad x - 1 = 7k \quad \Leftrightarrow \quad x = 7k + 1$$

Les solutions sont donc de la forme : $\begin{cases} x = 7k + 1 \\ y = 5k \end{cases}$, $k \in \mathbb{Z}$

B. Corollaire du théorème de Gauss

PROPRIÉTÉ

Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a.

REMARQUE : La preuve du corollaire du théorème de Gauss fait l'objet de l'exercice 40 p 14.

Exemple Si 5 et 12 divisent a, comme 5 et 12 sont premiers entre eux, $5 \times 12 = 60$ divise a.

C. Propriétés

Ces propriétés découlent du théorème de Bézout et de Gauss.

PROPRIÉTÉ

Soit a et b deux entiers non nuls, d leur pgcd et m leur ppcm.
1) Il existe deux entiers a' et b' premiers entre eux tels que : $a = da'$ et $b = db'$.
2) On a les relations suivantes : $m = da'b'$ et $ab = md$.

PREUVE
1) Dans la première relation a' et b' sont premiers entre eux car sinon d ne serait pas le plus grand diviseur commun.
2) Soit M un multiple de a et de b, donc il existe deux relatifs k_1 et k_2 tels que : $M = k_1a = k_2b$
Comme $a = da'$ et $b = db'$ on en déduit que : $k_1a = k_2b \Leftrightarrow k_1a' = k_2b'$.
Donc b' divise k_1a' or $\text{pgcd}(a', b') = 1$ d'après le théorème de Gauss, b' divise k_1. Il existe donc un relatif k_3 tel que $k_1 = k_3b'$.
En conséquence $M = k_1a = k_3b'a$.
Le plus petit multiple commun est donc obtenu en prenant $k_3 = 1$, on a alors $m = b'a = da'b'$
On en déduit alors : $md = d^2a'b' = ab$

5. Équation diophantienne *ax + by = c*

A. Définition et existence

DÉFINITION

Une équation diophantienne est une équation à coefficients entiers dont on cherche les solutions entières. Soient a, b et c trois entiers relatifs, les équations diophantiennes du premier degré sont du type : $ax + by = c$.

REMARQUE : Diophante d'Alexandrie est un mathématicien grec du III^e siècle de notre ère.

PROPRIÉTÉ

Une équation diophantienne du premier degré, de la forme $ax + by = c$, où a, b et c sont des entiers relatifs, admet des solutions si et seulement si c est un multiple du $\text{pgcd}(a, b)$

PREUVE Cela découle directement du corollaire du théorème de Bézout.

Exemple L'équation $17x - 33y = 1$ admet des solutions car $\text{pgcd}(17, 33) = 1$.

B. Résolution

MÉTHODE 4 Résoudre une équation du type *ax + by = c*

► Ex. 45 p. 14

Exercice d'application Déterminer l'ensemble des solutions de l'équation (E) $17x - 33y = 1$.

Correction

1) On cherche une solution particulière de (E). Ici, il existe une solution évidente le couple (2,1) car $17 \times 2 - 33 \times 1 = 34 - 33 = 1$.

2) On recherche ensuite la solution générale de (E).

On a : $\begin{cases} 17x - 33y = 1 \\ 17(2) - 33(1) = 1 \end{cases}$ par soustraction termes à termes des deux égalités, on obtient :

$$17(x-2) - 33(y-1) = 0 \Leftrightarrow 17(x-2) = 33(y-1) \quad (E')$$

33 divise $17(x-2)$ or le $\text{pgcd}(17,33) = 1$, d'après le théorème de Gauss, 33 divise $(x-2)$. On a donc : $x - 2 = 33k$, $k \in \mathbb{Z}$. En remplaçant dans (E'), on trouve $y - 1 = 17k$.

3) Les solutions de (E) sont de la forme : $\begin{cases} x = 2 + 33k \\ y = 1 + 17k \end{cases}$, $k \in \mathbb{Z}$

Exercice d'application Déterminer l'ensemble des solutions de l'équation (E_1) $15x + 8y = 5$.

Correction

1) L'équation (E_1) admet des solutions car 5 est un multiple du $\text{pgcd}(15,8) = 1$.

2) On cherche une solution particulière à l'équation (E_2) : $15x + 8y = 1$.
$(-1\,;\,2)$ est solution évidente à (E_2) car : $15 \times (-1) + 8 \times 2 = -15 + 16 = 1$.

3) En multipliant par 5, on trouve alors une solution particulière à (E_1). Le couple $(-5\,;\,10)$ est solution de (E_1).

4) On recherche ensuite la solution générale de (E_1).

On a : $\begin{cases} 15x + 8y = 5 \\ 15(-5) + 8(10) = 5 \end{cases}$ par soustraction termes à termes des deux égalités, on obtient :

$$15(x+5) + 8(y-10) = 0 \Leftrightarrow 15(x+5) = 8(10-y) \quad (E_2)$$

8 divise $15(x+5)$ or le $\text{pgcd}(15,8) = 1$, d'après le théorème de Gauss, 8 divise $(x+5)$. On a donc : $x + 5 = 8k$, $k \in \mathbb{Z}$. En remplaçant dans l'équation (E_2), on trouve $10 - y = 15k$.

5) Les solutions de (E_1) sont de la forme : $\begin{cases} x = -5 + 8k \\ y = 10 - 15k \end{cases}$, $k \in \mathbb{Z}$

S'entraîner

Activités mentales

1 Déterminer de tête et à l'aide des règles de divisibilité, les pgcd des entiers suivants :

1) 12 et 42.
2) 45 et 105.
3) 92 et 69.
4) 72 et 108.

2 Sur un vélodrome, deux cyclistes partent en même temps d'un point M et roulent à vitesse constante.
Le coureur A boucle le tour en 35 secondes et le coureur B en 42 secondes.
Au bout de combien de temps le coureur A aura-t-il un tour d'avance sur le coureur B ?

3

1) On veut découper un rectangle de 24 cm sur 40 cm en carrés dont le côté est le plus grand possible, sans perte.
   Quel doit-être le côté du carré ?
2) On dispose d'un grand nombre de rectangles du type précédent que l'on veut assembler bord à bord pour former un carré le plus petit possible.
   Quel doit être me côté du carré ?

4 Utiliser l'algorithme d'Euclide pour trouver le pgcd des nombres suivants :

1) 78 et 108.
2) 144 et 840.
3) 202 et 138.
4) 441 et 777.

5 Montrer que deux entiers naturels consécutifs non nuls sont premiers entre eux.

6 En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs (x, y) qui vérifient les équations suivantes :

1) $5(x+3) = 4y$
2) $41x + 9y = 0$

7 Trouver un couple d'entier relatif $(x; y)$ qui vérifie l'équation : $7x + 5y = 1$.

8 Existe-il des couples d'entiers (x, y) solutions de chacune des équations suivantes :

1) $37x + 25y = 1$
2) $51x + 39y = 1$
3) $51x + 39y = 2016$

PGCD-PPCM

9 Dresser la liste des diviseurs positifs de 72 et de 60. En déduire leur pgcd. Quel est leur ppcm ?

10 Si, en un point donné du ciel, un astre A apparaît tous les 28 jours et un astre B tous les 77 jours, avec quelle périodicité les verra-t-on simultanément en ce point ?

11 Déterminer tous les entiers naturels n inférieurs à 200 tels que : $\text{pgcd}(n, 324) = 12$.

12 ALGO
a et b sont deux naturels non nuls tels que $a > b$.

1) Démontrer que : $\text{pgcd}(a\ ,\ b) = \text{pgcd}(a - b\ ,\ b)$.
2) Calculer les pgcd des entiers suivants par cette méthode, répétée autant de fois que nécessaire :
   a) 308 et 165.
   b) 1 008 et 308.
   c) 735 et 210.
3) Écrire un algorithme permettant d'automatiser cette propriété pour calculer le pgcd de deux entiers. Tester-le à l'aide des questions de la question 2).

Algorithme d'Euclide

13 ► MÉTHODE 1 p. 6
Utiliser l'algorithme d'Euclide pour trouver le pgcd des nombres suivants :

1) 441 et 777.
2) 2004 et 9185.

14 Utiliser l'algorithme d'Euclide pour trouver le pgcd, puis en déduire le ppcm des nombres suivants :

1) 2012 et 7545.
2) 1386 et 546.

15 Utiliser l'algorithme d'Euclide pour trouver le pgcd, puis en déduire le ppcm des nombres suivants :

1) 4935 et 517.
2) 1064 et 700.

16 Les entiers suivants sont-ils premiers entre eux ?

1) 4847 et 5633.
2) 5617 et 813.

17 Si on divise 4294 et 3521 par un même entier positif, on obtient respectivement 10 et 11 comme reste. Quel est cet entier ?

18 En divisant 1 809 et 2 527 par un même entier naturel, les restes sont respectivement 9 et 7. Quel est le plus grand nombre que l'on peut obtenir comme diviseur ?

Relation entre PGCD et PPCM

19 **Vrai ou faux**

Si $\text{ppcm}(a,b) = ab$, alors a et b sont premiers entre eux. Justifier.

20 a, b et c sont des entiers naturels tels que : $\text{pgcd}(a,b) = \text{pgcd}(a,c)$.

A-t-on alors $\text{ppcm}(a,b) = \text{ppcm}(a,c)$? Justifier.

21 Résoudre dans $\mathbb{N}^2$ les systèmes suivants. On posera $d = \text{pgcd}(x,y)$ et $m = \text{ppcm}(x,y)$ et on donnera la réponse sous forme d'un tableau.

1) $\begin{cases} xy = 1512 \\ \text{ppcm}(x,y) = 252 \end{cases}$ **2)** $\begin{cases} xy = 300 \\ \text{ppcm}(x,y) = 60 \end{cases}$

22 Soit a et b deux naturels tels que $a < b$.

Déterminer a et b tels que : $\text{pgcd}(a,b) = 6$ et $\text{ppcm}(a,b) = 102$.

23 Soient x et y deux entiers naturels non nul.

On pose $m = \text{ppcm}(x,y)$ et $d = \text{pgcd}(x,y)$.

1) Quelle relation existe-t-il entre m et d ?

2) Résoudre dans $\mathbb{N}^2$, $m - 9d = 13$.

(On pourra donner les solutions sous forme d'un tableau).

24 Déterminer tous les couples $(a,b) \in \mathbb{N}^2$ dont $m = \text{ppcm}(a,b)$ et $d = \text{pgcd}(a,b)$ vérifient la relation :

$$8m = 105d + 30$$

25 n est un entier relatif quelconque. On pose :

$$A = n - 1 \quad \text{et} \quad B = n^2 - 3n + 6$$

1) a) Démontrer que le pgcd de A et de B est égal au pgcd de A et de 4.

b) Déterminer, selon les valeurs de l'entier n, le pgcd de A et de B.

2) Pour quelles valeurs de l'entier relatif n, $n \neq 1$, $\dfrac{n^2 - 3n + 6}{n - 1}$ est-il un entier relatif ?

26 On considère l'équation (E) : $x^2 - 52x + 480 = 0$, où x est un entier naturel.

Peut-on affirmer : « Il existe deux entiers naturels non nuls dont le pgcd et le ppcm sont solutions de l'équation (E). » ? Justifier.

27 On note n un naturel non nul, $a = 3n + 1$ et $b = 5n - 1$.

1) Montrer que le pgcd(a,b) est un diviseur de 8.

2) Pour quelles valeurs de n, le pgcd(a,b) est-il égal à 8 ?

Théorème de Bézout

28 Soit l'égalité de Bézout : « Soit a et b deux entiers non nuls et D leur pgcd. Il existe un couple d'entiers relatifs telle que $au + bv = D$ ».

Démontrer le théorème de Bézout « a et b sont premiers entre eux si, et seulement si, il existe un couple d'entiers relatifs telle que $au + bv = 1$ ».

29 ► **MÉTHODE 2** p. 8

Démontrer que, pour tout relatif k, $(7k + 3)$ et $(2k + 1)$ sont premiers entre eux.

30 n est un entier naturel, $a = 7n + 4$ et $b = 5n + 3$.

Montrer, pour tout n, que a et b sont premiers entre eux.

31 Démontrer que pour tout relatif n, les entiers $(14n + 3)$ et $(5n + 1)$ sont premiers entre eux. En déduire le pgcd$(87\ ,\ 31)$

32 Prouver que la fraction $\dfrac{n}{2n + 1}$ est irréductible pour tout entier naturel n.

33 Prouver que la fraction $\dfrac{2n + 1}{n(n + 1)}$ est irréductible pour tout entier naturel n.

34 La fraction $\dfrac{n^3 + n}{2n + 1}$ est-elle irréductible pour tout entier naturel n ?

35 ► **MÉTHODE 3** p. 8

Montrer que 17 et 40 sont premiers entre eux puis déterminer un couple d'entiers relatifs (x,y) tel que : $17x - 40y = 1$.

36 Montrer que 23 et 26 sont premiers entre eux puis déterminer un couple d'entiers relatifs (x,y) tel que : $23x + 26y = 1$.

37 L'équation $6x + 3y = 1$ admet-elle des solutions entières ? Même question avec $7x + 5y = 1$?

S'entraîner

38 Montrer que 221 et 331 sont premiers entre eux puis déterminer un couple d'entiers relatifs (x, y) tel que : $221x - 331y = 1$.

39 **Vrai ou faux**

S'il existe deux entiers relatifs u et v tel que $au + bv = 3$ alors le pgcd de a et de b est égal à 3. Justifier.

Théorème de Gauss

40 En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs (a, b) qui vérifient :

$$33a - 45b = 0$$

41

1) En utilisant le théorème de Gauss, déterminer les couples d'entiers relatifs (x, y) qui vérifient :

$$7(x - 3) = 5(y - 2)$$

2) De la question précédente, déterminer les entiers naturels x tels que : $7x \equiv 1\ (5)$.

42 En utilisant le théorème de de Gauss, démontrer le corollaire du théorème de Gauss :
« Si b et c divisent a et si b et c sont premiers entre eux, alors bc divise a ».

43 Montrer que si $n \equiv 0\ (8)$ et $n \equiv 0\ (9)$ alors $n \equiv 0\ (72)$.

Équations du type *ax + by = c*

44 Soit l'égalité de Bézout : « Soit a et b deux entiers non nuls et D leur pgcd. Il existe un couple d'entiers relatifs telle que $au + bv = D$ ».
Démontrer le corollaire du théorème de Bézout : « L'équation $ax + by = c$ admet des solutions entières si, et seulement si, c est un multiple du pgcd(a, b) ».

45 ► MÉTHODE 4 p. 11

Soit l'équation $4x - 3y = 2$.

1) Déterminer une solution particulière entière à cette équation.
2) Déterminer l'ensemble des solutions entières.

46 Soit l'équation $3x - 4y = 6$.

1) Déterminer une solution particulière entière à cette équation.
2) Déterminer l'ensemble des solutions entières.

47 Soit l'équation $5x + 8y = 2$.

1) Déterminer une solution particulière entière à cette équation.
2) Déterminer l'ensemble des solutions entières.

48 Soit l'équation $13x - 23y = 1$.

1) Déterminer une solution particulière entière à l'aide de l'algorithme d'Euclide à cette équation.
2) Déterminer l'ensemble des solutions entières.

49

1) Déterminer l'ensemble des couples $(x; y)$ de nombres entiers relatifs, solution de l'équation :

$$\text{(E)} \ : \ 8x - 5y = 3$$

2) Soit m un nombre entier relatifs tel qu'il existe un couple $(p; q)$ de nombres entiers vérifiant :
$m = 8p + 1$ et $m = 5q + 4$.
Montrer que le couple (p, q) est solution de l'équation (E).
3) Déterminer le plus petit de ces nombres entiers m supérieurs à 2 000.

50

1) On considère l'équation (E) à résoudre dans $\mathbb{Z}$:

$$7x - 5y = 1$$

a) Vérifier que le couple (3 ; 4) est solution de (E).
b) Montrer que le couple d'entiers $(x\ ;\ y)$ est solution de (E) si et seulement si $7(x - 3) = 5(y - 4)$.
c) Montrer que les solutions entières de l'équation (E) sont exactement les couples $(x\ ;\ y)$ d'entiers relatifs tels que :

$$\begin{cases} x = 5k + 3 \\ y = 7k + 4 \end{cases} \text{ où } k \in \mathbb{Z}.$$

2) Une boîte contient 25 jetons, des rouges, des verts et des blancs. Sur les 25 jetons il y a x jetons rouges et y jetons verts. Sachant que $7x - 5y = 1$, quels peuvent être les nombres de jetons rouges, verts et blancs ?

BAC

51 Antilles-Guyane juin 2014

En montagne, un randonneur a effectué des réservation dans deux types d'hébergement :
L'hébergement A et l'hébergement B.
Une nuit en hébergement A coûte 24 € et une nuit en hébergement B coûte 45 €.
Il se rappelle que le coût total de sa réservation est de 438 €.

On souhaite retrouver les nombres x et y de nuitées passées respectivement en hébergement A et en hébergement B

1) a) Montrer que les nombres x et y sont respectivement inférieurs ou égaux à 18 et 9.

b) Recopier et compléter les pointillés de l'algorithme suivant afin qu'il affiche les couples $(x\ ;\ y)$ possibles.

```
1.  Liste des variables utilisées
2.    x, y : entiers
3.  Traitements et affichage
4.    Pour x variant de 0 à ... faire
5.      Pour y variant de 0 à ... faire
6.        Si  ...  Alors
7.          Afficher la valeur x, y
8.        Fin Si
9.      Fin Pour
10.   Fin Pour
```

2) Justifier que le coût total de la réservation est un multiple de 3.

3) a) Justifier que l'équation $8x + 15y = 1$ admet pour solution au moins un couple d'entiers relatifs.

b) Déterminer une telle solution.

c) Résoudre l'équation (E) : $8x + 15y = 146$ où x et y sont des nombres entiers relatifs.

4) Le randonneur se souvient avoir passé au maximum 13 nuits en hébergement A.
Montrer alors qu'il peut retrouver le nombre exact de nuits passées en hébergement A et celui des nuits passées en hébergement B.
Calculer ces nombres.

52 Métropole juin 2011

Partie A - Restitution organisée de connaissances

On rappelle ci-dessous le théorème de Bézout et le théorème de Gauss.
Théorème de Bézout :
« Deux entiers relatifs a et b sont premiers entre eux si et seulement si, il existe un couple (u, v) d'entiers relatifs vérifiant $au + bv = 1$. »
Théorème de Gauss :
« Soient a, b, c des entiers relatifs. Si a divise le produit bc et si a et b sont premiers entre eux, alors a divise c. »

1) En utilisant le théorème de Bézout, démontrer le théorème de Gauss.

2) Soient p et q deux entiers naturels tels que p et q sont premiers entre eux.
Déduire du théorème de Gauss que, si a est un entier relatif, tel que $a \equiv 0\ (p)$ et $a \equiv 0\ (q)$, alors $a \equiv 0\ (pq)$.

Partie B - Restes chinois

On se propose de déterminer l'ensemble $\mathscr{S}$ des entiers relatifs n vérifiant le système :

$$\begin{cases} n \equiv 9\ (17) \\ n \equiv 3\ (5) \end{cases}$$

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

a) Justifier l'existence d'un tel couple (u, v).

b) On pose $n_0 = 3 \times 17u + 9 \times 5v$.
Démontrer que n_0 appartient à $\mathscr{S}$.

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

2) Caractérisation des éléments de $\mathscr{S}$.

a) Soit n un entier relatif appartenant à $\mathscr{S}$.
Démontrer que $n - n_0 \equiv 0\ (85)$.

b) En déduire qu'un entier relatif n appartient à $\mathscr{S}$ si et seulement si n peut s'écrire sous 1a forme $n = 43 + 85k$ où k est un entier relatif.

3) Application
Zoé sait qu'elle a entre 300 et 400 jetons. Si elle fait des tas de 17 jetons, il lui en reste 9. Si elle fait des tas de 5 jetons, il lui en reste 3.

Combien a-t-elle de jetons ?

53 N^lle Calédonie 2007 (partiel)

1) Dans cette question x et y désignent des entiers relatifs.

a) Montrer que l'équation (E) : $65x - 40y = 1$ n'a pas de solution.

b) Montrer que l'équation (E') : $17x - 40y = 1$ admet au moins une solution.

c) Déterminer à l'aide de l'algorithme d'Euclide un couple d'entiers relatifs solution de l'équation (E').

d) Résoudre l'équation (E').
En déduire qu'il existe un unique naturel $x_0 < 40$ tel que : $17x_0 \equiv 1\ (40)$.

2) Pour tout naturel a, démontrer que si $a^{17} \equiv b\ (55)$ et si $a^{40} \equiv 1\ (55)$, alors $b^{33} \equiv a\ (55)$.

54 Antilles-Guyane 2015

Partie A

Pour deux entiers naturels non nuls a et b, on note $r(a, b)$ le reste dans la division euclidienne de a par b.
On considère l'algorithme suivant :

```
1.  Liste des variables utilisées
2.      c : entier naturel
3.      a, b : entiers naturels non nuls
4.  Entrées
5.      Saisir a
6.      Saisir b
7.  Traitements
8.      Donner à a la valeur de r(a, b)
9.      Tant que (c ≠ 0) faire
10.         Donner à a la valeur de b
11.         Donner à b la valeur de c
12.         Donner à c la valeur de r(a, b)
13.     Fin Tant que
14. Affichage
15.     Afficher la valeur b
```

1) Faire fonctionner cet algorithme avec $a = 26$ et $b = 9$ en indiquant les valeurs de a, b et c à chaque étape.

2) Cet algorithme donne en sortie le pgcd des entiers naturels non nuls a et b.
Le modifier pour qu'il indique si deux entiers naturels non nuls a et b sont premiers entre eux ou non.

Partie B

À chaque lettre de l'alphabet on associe grâce au tableau ci-dessous un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :
Étape 1 : on choisit deux entiers naturels p et q compris entre 0 et 25.
Étape 2 : à la lettre que l'on veut coder, on associe l'entier x correspondant dans le tableau ci-dessus.
Étape 3 : on calcule l'entier x' défini par les relations

$$x' \equiv px + q\ (26) \quad \text{et} \quad 0 \leqslant x' \leqslant 25$$

Étape 4 : à l'entier x', on associe la lettre correspondante dans le tableau.

1) Dans cette question, on choisit $p = 9$ et $q = 2$.

a) Démontrer que la lettre V est codée par la lettre J.

b) Citer le théorème qui permet d'affirmer l'existence de deux entiers relatifs u et v tels que : $9u + 26v = 1$. Donner sans justifier un couple (u, v) qui convient.

c) Démontrer que $x' \equiv 9x + 2\ (26)$ équivaut à : $x \equiv 3x' + 20\ (26)$.

d) Décoder la lettre R.

2) Dans cette question, on choisit $q = 2$ et p est inconnu.
On sait que J est codé par D.
Déterminer la valeur de p (on admettra que p est unique).

3) Dans cette question, on choisit $p = 13$ et $q = 2$. Coder les lettres B et D. Que peut-on dire de ce codage ?

Autres

55 Carrelage d'une pièce

Pour carreler une pièce rectangulaire mesurant 4,18 m sur 5,67 m, un carreleur propose à des propriétaires le choix entre deux modèles de dalles carrées.

1) Le premier modèle a 29 cm de côté et coûte 2,30 € l'unité.
   Avec ce modèle, il n'utilise que des dalles entières et il complète avec du joint autour de chaque dalle.
   a) Calculer le nombre maximal de dalles que l'on peut poser dans la largeur de la pièce.
   b) Calculer le nombre maximal de dalles que l'on peut poser dans la longueur de la pièce.
   c) Les joints autour des dalles auront-ils tous la même largeur ?
   Si oui, quelle est cette largeur ?
2) Le deuxième modèle a 36 cm de côté et coûte 3,10 € l'unité.
   Avec ce modèle-là, il est préconisé des joints de 0,6 cm et le carreleur est alors dans l'obligation de couper des dalles et les découpes ne sont pas réutilisées. Calculer le nombre de dalles nécessaires.
3) Quel sera le choix le moins coûteux pour l'achat des dalles ?

56 Vrai-Faux

Pour chacune des 4 propositions, indiquer si elle est vraie ou fausse et donner une démonstration de la réponse choisie.

1) **Proposition 1 :** $\forall n \in \mathbb{N}^*$, $3n$ et $2n+1$ sont premiers entre eux.
2) On appelle S l'ensemble des couples $(x;y)$ d'entiers relatifs solutions de l'équation $3x-5y=2$.
   Proposition 2 : « L'ensemble S est l'ensemble des couples $(5k-1\ ;\ 3k-1)$ où k est un entier relatif. »
3) Soient a et b deux entiers naturels.
   Proposition 3 : « S'il existe deux entiers relatifs u et v tels que $au+bv=2$ alors le pgcd de a et b est égal à 2 ».
4) On considère l'équation (E) : $x^2-52x+480=0$, où x est un entier naturel.
   Proposition 4 : « Il existe deux entiers naturels non nuls dont le pgcd et le ppcm sont solutions de l'équation (E). »

57 Un problème du VIIIe siècle

1) On considère l'équation (E) : $8x+5y=1$, où $(x\ ;\ y)$ est un couple de nombres entiers relatifs.
   a) Donner une solution particulière de l'équation (E).
   b) Résoudre l'équation (E).
2) Soit N un nombre naturel tel qu'il existe un couple $(a\ ;\ b)$ de nombres entiers vérifiant :
$$\begin{cases} N=8a+1 \\ N=5b+2. \end{cases}$$
   a) Montrer que le couple $(a\ ;\ -b)$ est solution de (E).
   b) Quel est le reste, dans la division de N par 40 ?

3) a) Résoudre l'équation $8x+5y=100$, où $(x\ ;\ y)$ est un couple de nombres entiers relatifs.
   b) Au VIIIe siècle, un groupe composé d'hommes et de femmes a dépensé 100 pièces de monnaie dans une auberge. Les hommes ont dépensé 8 pièces chacun et les femmes 5 pièces chacune. Combien pouvait-il y avoir d'hommes et de femmes dans le groupe ?

58 Restes chinois bis

On se propose de résoudre dans $\mathbb{Z}$ le système :
$$\begin{cases} N \equiv 5\ [13] \\ N \equiv 1\ [17] \end{cases}$$

1) Vérifier que 239 est solution de ce système.
2) Soit N un entier relatif solution de ce système.
   Démontrer que N peut s'écrire sous la forme :
   $N=1+17x=5+13y$ où x et y sont deux entiers relatifs vérifiant la relation $17x-13y=4$.
3) Résoudre l'équation $17x-13y=4$ où x et y sont des entiers relatifs.
4) En déduire qu'il existe un entier relatif k tel que $N=18+221k$.

59 Conjonction de comètes

Le but est de déterminer l'ensemble $\mathscr{S}$ des entiers relatifs n vérifiant le système :
$$\begin{cases} n \equiv 13\ [19] \\ n \equiv 6\ [12] \end{cases}$$

1) Recherche d'un élément de $\mathscr{S}$.

On désigne par (u, v) un couple d'entiers relatifs tel que $19u + 12v = 1$.

a) Justifier l'existence d'un tel couple (u, v).

b) On pose $n_0 = 6 \times 19u + 13 \times 12v$.
Démontrer que n_0 appartient à $\mathscr{S}$.

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

2) Caractérisation des éléments de $\mathscr{S}$.

a) Soit n un entier relatif appartenant à $\mathscr{S}$.
Démontrer que $n - n_0 \equiv 0\ (228)$.

b) En déduire qu'un entier relatif n appartient à $\mathscr{S}$ si et seulement si n peut s'écrire sous 1a forme $n = -6 + 228k$ où k est un entier relatif.

3) Application :
La comète A passe tous les 19 ans et apparaîtra la prochaine fois, dans 13 ans.
La comète B passe tous les 12 ans et apparaitra la prochaine fois, dans 6 ans.
Dans combien d'années pourra-t-on observer les deux comètes la même année ?

60 Algorithme et équation diophantienne

On considère l'algorithme suivant, où A et B sont des entiers naturels tels que $A < B$:

```
1.  Liste des variables utilisées
2.    A, B, C, D : entiers
3.  Entrées
4.    Saisir X, Y tel que A < B
5.  Traitements
6.    Donner à D la valeur de B − A
7.    Tant que (D > 0) faire
8.      Donner à B la valeur de A
9.      Donner à A la valeur de D
10.     Si B > A Alors
11.       Donner à D la valeur de B − A
12.     Sinon
13.       Donner à D la valeur de A − B
14.     Fin Si
15.   Fin Tant que
16. Affichage
17.   Afficher la valeur A
```

1) On entre $A = 12$ et $B = 14$.
En remplissant le tableau suivant, déterminer la valeur affichée par l'algorithme.

A	B	D
12	14	

2) Que calcule cet algorithme ?

3) a) Montrer que 221 et 331 sont premiers entre eux.

b) Justifier que l'équation (E) $221x - 331y = 1$ admet des solutions entières.

c) Déterminer une solution particulière de l'équation (E).
(On pourra éventuellement remonter l'algorithme d'Euclide.)

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

4) On considère les suites d'entiers naturels (u_n) et (v_n) définies pour tout entier naturel n par

$$u_n = 2 + 221n \quad \text{et} \quad \begin{cases} v_0 = 3 \\ v_{n+1} = v_n + 331 \end{cases}$$

a) Quelle est la nature de la suite (v_n) ?
En déduire l'expression de v_n en fonction de l'entier naturel n.

b) Déterminer tous les couples d'entiers naturels $(p\ ;\ q)$ tels que
$u_p = v_q$, $0 \leqslant p \leqslant 500$ et $0 \leqslant q \leqslant 500$.

Je teste mes connaissances

À la fin de ce chapitre, je dois être capable de :

- Calculer un pgcd par l'algorithme d'Euclide.
- Déduire le ppcm à partir du pgcd.
- Connaître l'énoncé de l'égalité de Bézout.
- Connaître le théorème et le corollaire de Bézout.
- Connaître le théorème et le corollaire de Gauss.
- Trouver une solution particulière à l'équation : $ax + by = c$.
- Trouver toutes les solutions dans $\mathbb{Z}^2$ de l'équation : $ax + by = c$.

QCM d'auto-évaluation

Des ressources numériques pour préparer le chapitre sur manuel.sesamath.net

Pour chaque question, plusieurs réponses sont proposées. Déterminer la réponse exacte en la justifiant.

61 Le $\text{pgcd}(25\,176\ ,\ 42\,722) = 82$. Combien de divisions, à l'aide de l'algorithme d'Euclide, sont-elles nécessaires jusqu'à obtenir un reste nul ?

(a) 6 (b) 7 (c) 8 (d) 9

62 a et b sont deux entiers naturels tels que : $\text{pgcd}(a, b) = 7$.
Dans l'algorithme d'Euclide, les quotients successifs sont 3, 1, 1, 2 (comprenant la dernière division de reste nul). Alors :

(a) $(a, b) = (35, 63)$ (b) $(a, b) = (35, 126)$ (c) $(a, b) = (25, 126)$

Le ppcm des entiers a et b est alors :

(a) 882 (b) 4 410 (c) 630

63 Pour tout entier n, on pose $a = 3n - 5$ et $b = 2n - 7$.

(a) a et b sont premiers entre eux
(b) Le $\text{pgcd}(a, b) = 11$
(c) Tout diviseurs communs à a et b divise 11
(d) a et b ne sont pas premiers entre eux.

64 Soit n un entier naturel. Laquelle des fractions suivantes est irréductible pour tout n ?

(a) $\dfrac{3n}{2n+1}$ (b) $\dfrac{n+8}{2n+5}$ (c) $\dfrac{3n^2}{2n^2+n}$ (d) $\dfrac{n}{(2n+1)(3n+1)}$

65 L'équation diophantienne $5x - 8y = 1$ admet comme solutions des couples d'entiers relatifs qui sont :

(a) toujours premier entre eux.
(b) parfois premiers entre eux.
(c) jamais premiers entre eux
(d) rien du tout. On ne peut pas déterminer si les entiers sont premiers entre eux ou non.

66 Un nombre est divisible par 15 et par 24, alors ce nombre est divisible par

(a) 360 (b) 120 (c) 90 (d) 72

67 Soit k un entiers relatif. L'équation $5(x-2)=7k$ a pour solution :

(a) $x \equiv 2\ (5)$ (b) $x \equiv 5\ (7)$ (c) $x \equiv 2\ (7)$ (d) $x \equiv 0\ (7)$

68 Soient a, b, c trois des entiers relatifs et n un entier naturel ($n \geqslant 2$).

La proposition : « Si $ac \equiv bc\ (n)$ alors $a \equiv b\ (n)$ »

(a) est toujours vraie.

(b) est vraie si c et n sont premiers entre eux.

(c) est vraie si a et b sont premiers entre eux.

(d) n'est jamais vraie.

69 Soit l'équation diophantienne (E) : $27x+25y=1$

(a) $(48\ ,-71)$ est solution de (E).

(b) (E) admet un couple d'entiers naturels comme solution.

(c) $(25\ ,\ 37)$ est solution de (E).

(d) (E) n'admet pas de solution.

70 L'équation diophantienne : $17x-13y=2$ admet

(a) aucune solution.

(b) comme solutions : $\begin{cases} x=-6+13k \\ y=-8+17k \end{cases}$, $k \in \mathbb{Z}$.

(c) comme solutions : $\begin{cases} x=7+26k \\ y=9+34k \end{cases}$, $k \in \mathbb{Z}$.

(d) comme solutions : $\begin{cases} x=7+13k \\ y=9-17k \end{cases}$, $k \in \mathbb{Z}$.

Dans les exercices suivants, plusieurs réponses sont proposées. Déterminer celles qui sont exactes. Justifier.

71 Relever les affirmations vraies.

(a) Si le $\text{pgcd}(a,b)=1$ alors le $\text{pgcd}(a+b\ ,\ b)=1$.

(b) Il existe deux naturels a et b tels la somme vaut 150 et le $\text{pgcd}(a,b)=8$.

(c) Deux nombres impairs consécutifs sont premiers entre eux.

(d) L'équation $51x+39y=2016$ admet des solutions entières.

72 Dans un chiffrement affine, la fonction de codage est définie par la fonction $f(x)=17x+22$ (voir tableau de codage de l'activité 3 p.3).

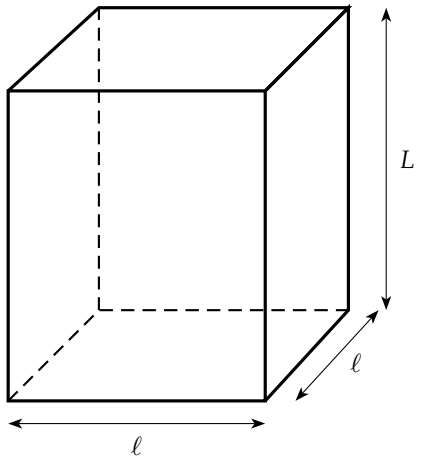
(a) Le codage de « HUIT » est « LYCA »

(b) Le message « PZWC » veut dire « VRAI »

(c) La seule solution dans $\mathbb{Z}^2$ de l'équation $17x-26y=1$ est (23,15)

(d) La fonction de décodage est : $f^{-1}(y)=23y+14$

TP 1 Boîtes dans une caisse



1) Soit B une boîte en forme de pavé droit de hauteur L, à base carrée de côté ℓ, où ℓ et L sont des entiers naturels non nuls tels que $\ell < L$. On veut remplir la boîte B avec des cubes tous identiques dont l'arête a est un entier naturel non nul (les cubes devant remplir complètement la boîte B sans laisser d'espace vide).

a) Dans cette question, $\ell = 882$ et $L = 945$. Quelle est la plus grande valeur possible pour a ? Quelles sont les valeurs possibles pour a ?

b) Dans cette question, le volume de la boîte B est $v = 77\,760$. On sait que, pour remplir la boîte B, la plus grande valeur possible de a est 12. Montrer qu'il y a exactement deux boîtes B possibles, dont on donnera les dimensions.

2) On veut remplir une caisse cubique C, dont l'arête c est un entier naturel non nul, avec des boîtes B toutes identiques telles que décrites dans la question 1 (Les boîtes B, empilées verticalement, doivent remplir complètement la caisse C sans laisser d'espace vide).

a) Dans cette question, $\ell = 882$ et $L = 945$. Quelle est la plus petite arête c pour la caisse C ? Quel est l'ensemble de toutes les valeurs possibles pour l'arête c ?

b) Dans cette question, le volume de la boîte B est 15 435. On sait que la plus petite arête possible pour la caisse C est 105.
Quelles sont les dimensions ℓ et L de la boîte B ?

TP 2 Conjonction de corps célestes

Un astronome a observé au jour J_0 le corps céleste A, qui apparaît périodiquement tous les 105 jours. Six jours plus tard ($J_0 + 6$), il observe le corps B, dont la période d'apparition est de 81 jours. On appelle J_1 le jour de la prochaine apparition simultanée des deux objets aux yeux de l'astronome.
Le but de cet exercice est de déterminer la date de ce jour J_1.

1) Soient u et v le nombre de périodes effectuées respectivement par A et B entre J_0 et J_1. Montrer que le couple $(u\,;\,v)$ est solution de l'équation (E_1) : $35x - 27y = 2$.

2) a) Déterminer un couple de relatifs $(x_0\,,\,y_0)$ solution particulière de l'équation (E_2) : $35x - 27y = 1$.

b) En déduire une solution particulière $(u_0\ ;\ v_0)$ de (E_1).

c) Déterminer toutes les solutions de l'équation (E_1).

d) Déterminer la solution $(u\ ;\ v)$ permettant de déterminer J_1.

3) a) Combien de jours s'écouleront entre J_0 et J_1 ?

b) Le jour J_0 était le mardi 7 décembre 1999, quelle est la date exacte du jour J_1 ? (L'année 2000 était bissextile.)

c) Si l'astronome manque ce futur rendez-vous, combien de jours devra t-il attendre jusqu'à la prochaine conjonction des deux astres ?

Portrait imaginaire d'Hypatie d'Alexandrie

Hypatie d'Alexandrie (vers 370 - 415)
Seule mathématicienne de l'antiquité. Elle écrit notamment des commentaires sur l'arithmétique de Diophante et sur les tables de Ptolémée.
Elle meurt malheureusement lapidée par des moines chrétiens fanatiques.

TP 3 Chiffrement de Hill

Partie A : Inverse de 23 modulo 26

Soit l'équation : (E) : $23x - 26y = 1$, où x et y désignent deux entiers relatifs.

1) Vérifier que le couple $(-9\ ;\ -8)$ est solution de l'équation (E).

2) Résoudre alors l'équation (E).

3) En déduire un entier a tel que $0 \leqslant a \leqslant 25$ et $23a \equiv 1 \pmod{26}$.

Partie B : Codage et décodage

Le chiffrement de Hill a été publié en 1929. C'est un chiffre polygraphique, c'est à dire qu'on ne chiffre pas les lettres les unes après le autres, mais par « paquets ». Soit un exemple « bigraphique », c'est à dire que les lettres sont regroupées deux à deux.

Étape 1 : On regroupe les lettres par 2. Chaque lettre est remplacée par un entier en utilisant le tableau ci-dessous :

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

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

On obtient des couples d'entiers $(x_1\ ;\ x_2)$ où x_1 correspond à la première lettre et x_2 correspond à la deuxième lettre.

Étape 2 : Chaque couple $(x_1\ ;\ x_2)$ est transformé en $(y_1\ ;\ y_2)$ tel que :

$$(S_1)\ \begin{cases} y_1 \equiv 11x_1 + 3x_2\ (26) \\ y_2 \equiv 7x_1 + 4x_2\ (26) \end{cases} \quad \text{avec } 0 \leqslant y_1 \leqslant 25 \text{ et } 0 \leqslant y_2 \leqslant 25.$$

Étape 3 Chaque couple $(y_1\ ;\ y_2)$ est transformé en un couple de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1. On regroupe ensuite les lettres.

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape1}}{\Longrightarrow} (19,4) \overset{\text{étape 2}}{\Longrightarrow} (13,19) \overset{\text{étape 3}}{\Longrightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1) Coder le mot ST.

2) On décide de construire un algorithme permettant d'aller plus vite.
On propose l'algorithme suivant :

1. *Liste des variables utilisées*
2. X, Y, Z, Y : entiers
3. *Entrées*
4. Saisir X, Y
5. *Traitements*
6. Donner à Z la valeur de $11X + 3Y$
7. Donner à T la valeur de $7X + 4Y$
8. Donner à Z la valeur de $Z - 26 \times \mathrm{E}\left(\frac{Z}{26}\right)$
9. Donner à T la valeur de $T - 26 \times \mathrm{E}\left(\frac{T}{26}\right)$
10. *Affichage*
11. Afficher la valeur Z, T

La fonction E( ) signifiant la partie entière.

a) Coder PALACE et RAPACE.

b) Que constatez-vous ?

3) On veut maintenant déterminer la procédure de décodage :

a) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_1), vérifie les équations du système :

$$(S_2)\quad \begin{cases} 23x_1 \equiv 4y_1 + 23y_2\ (26) \\ 23x_2 \equiv 19y_1 + 11y_2\ (26) \end{cases}$$

b) À l'aide de la partie A, montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_2), vérifie les équations du système :

$$(S_3)\quad \begin{cases} x_1 \equiv 16y_1 + y_2\ (26) \\ x_2 \equiv 11y_1 + 5y_2\ (26) \end{cases}$$

c) Montrer que tout couple $(x_1\ ;\ x_2)$ vérifiant les équations du système (S_3), vérifie les équations du système (S_1).

d) Écrire un algorithme sur le même principe que l'algorithme de chiffrage pour décoder un mot.

e) Décoder le mot : PFXXKNU.
Ce mot étant de 7 lettres, ajouter la lettre W à la fin du mot pour avoir des paquets de deux lettres. Le décodage terminé, on supprimera la lettre dont le code est W.

Récréation, énigmes

Repas gastronomique

28 personnes participent à un repas gastronomique. Le prix normal est de 26 € sauf pour les étudiants et les enfants qui paient respectivement 17 € et 13 €. La somme totale recueillie est de 613 €.
Calculer le nombre d'étudiants et d'enfants ayant participé au repas. Proposer un algorithme puis deux méthodes pour résoudre ce problème.

Jour et mois de naissance

En multipliant mon jour de naissance par 12 et mon mois de naissance par 31, j'obtiens 442.
Quelle est ma date de naissance ? On proposera un algorithme puis une méthode pour résoudre ce problème.
(On ne demande pas l'année, ouf !)

Théorème des restes chinois

« Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ? »

Le grand nom pour la résolution moderne de ce problème est évidemment celui de Carl Friedrich Gauss (1777-1855), à qui nous devons, bien au delà de la solution complète du problème des congruences simultanées, la définition des congruences et leur constitution en une nouvelle arithmétique, qui donnera naissance à la théorie des corps finis et notamment à son application contemporaine au cryptage.