CHAPITRE 2

PGCD Théorème de Bézout Théorème de Gauss

SÉQUENCE 1 PGCD de deux entiers naturels (page 40)

RÉSOLUTION DE PROBLÈMES

Problème 1

1. $945 = 882 + 63$ et $882 = 63 \times 14$.
Donc PGCD(945 ; 882) = 63 car d doit diviser 945 et 882 et la plus grande valeur de d est le PGCD des deux nombres.

2. a) • Si A = B, après un premier passage dans la boucle « Tant que », le reste R est nul. On obtient à l'affichage la valeur commune A.
• Si A < B, le premier quotient est nul, le reste est A, donc non nul. À l'issue d'un premier passage dans la boucle, A et B sont échangés : on repart donc avec A > B.

b) On affecte à R une valeur différente de zéro (ce qui se passe parfois à l'initialisation) afin de démarrer le passage effectif dans la boucle « Tant que ».

c) Si R ≠ 0, le couple (A ; B) est remplacé par le couple (B ; R). Or, dans ce cas là, PGCD(A ; B) = PGCD(B ; R).

Lorsque R est nul, c'est-à-dire lorsque B divise A, le PGCD de A et B est B, que l'on lit dans la mémoire A.

d)

A	B	Q	R
945	882	1	63
882	63	14	0

d est le dernier reste non nul :

$$d = \text{PGCD}(945 ; 882) = 63.$$

3. Les diviseurs de 63 sont : 1, 3, 7, 9, 21, 63.
Il n'y a pas d'autres solutions.

Problème 2

1. b) L' et ℓ' sont tels que : PGCD(L' ; ℓ') = 1.

2. L = 12 L' ; $\ell = 12\ell'$; ℓ^2L = 77 760.
Soit $144\,\ell'^2 \times 12\,L' = 77\,760$ et $\ell'^2 L' = 45 = 3^2 \times 5$.
D'où $\ell' = 1$ ou $\ell' = 3$; donc L' = 45 ou L' = 5.
Les couples (l ; L) sont : (12 ; 540) ou (36 ; 60).

EXERCICES Application (page 44)

1 **1.** Tout diviseur d de a et b divise toute combinaison linéaire de a et b ; par exemple :

$$2a - 5b = 2(5n + 1) - 5(2n - 1) = 7.$$

Donc d divise 7 et Δ a pour valeurs possibles 1 et 7.

2. a)

$n \equiv$	0	1	2	3	4	5	6
$a = 5n + 1 \equiv$	1	6	4	2	0	5	3
$b = 2n - 1 \equiv$	6	1	3	5	0	2	4

Donc $a \equiv 0 \pmod 7$ et $b = 0 \pmod 7$ si, et seulement si, $n = 7k + 4$.

b) Si $n = 7k + 4$ ($k \in \mathbb{N}$) ; PGCD$(a\ ;\ b) = 7$;
Si $n \neq 7k + 4$; PGCD$(a\ ;\ b) = 1$.

2 **1.** Si d divise a et b alors d divise $5b - a$, soit d divise 3.

2.

$n \equiv$	0	1	2
$n^2 \equiv$	0	1	1
$a \equiv$	2	1	1
$b \equiv$	1	2	2

3. a et b ne sont pas congru 0 modulo 3.
Donc PGCD$(a\ ;\ b) = 1$ et a et b sont premiers entre eux.

3 $4\,294 = nq_1 + 10$ et $3\,521 = nq_2 + 11$.
Soit $nq_1 = 4\,284$ et $nq_2 = 3\,510$.
n est un diviseur commun à 4 284 et 3 510, donc un diviseur de leur PGCD avec $n > 11$.

	1	4	1	1	6	1	2
4 284	3 510	774	414	360	54	36	18
774	414	360	54	36	18	0	

Comme n divise 18 et $n > 11$, alors $n = 18$.

4 **a)** $4b + r_1$; $b = r_1 + r_2$; $r_1 = 3\,r_2 + r_3$.
$r_2 = 2\,r_3$ et $r_3 = 36$.
On en déduit successivement r_2, r_1, b et a.
Soient $a = 1\,548$ et $b = 324$.

5 **a)** PGCD$(a\ ;\ b) = 12$; donc les diviseurs communs sont $\{1, 2, 3, 4, 6, 12\}$.

b) PGCD$(37\,425\ ;\ 3\,493) = 499$.
Ses diviseurs sont $\{1\ ;\ 499\}$.

6 **1. a)**

	1	3
484	363	121
121	0	

PGCD$(484\ ;\ 363) = 121 = 484 - 363$.

b) Donc $(484\ ;\ 363) \in \mathcal{S}$.

2. Tout diviseur d commun à $(n + 1)$ et n divise leur différence $(n + 1) - 4 = 1$.
Donc PGCD$(n + 1\ ;\ n) = 1$ et $(n + 1\ ;\ n) \in \mathcal{S}$.

3. $x = (x - y)q$ et $y = (x - y)p$ avec $(x - y) = (x - y)(q - p)$.
Donc $q = p + 1$. De plus, p et $p + 1$ sont premiers entre eux donc :

$$x = (x - y)(p + 1) \quad \text{et} \quad y = (x - y)p.$$

7 $a = 12a'$ et $b = 12b'$ avec PGCD$(a'; b') = 1$;
donc $a' = 50$ et $260 < 12b' < 300$, d'où :

$$b' \in \{22\ ;\ 23\ ;\ 24\}.$$

Or, a' et b' étant premiers entre eux, il en résulte que $b' = 23$ et $b = 276$.

8 $a = 20a'$ et $320 = 20 \times 16$, donc $a' < 16$.
a' est premier avec 16, donc :

$$a' \in \{1\ ;\ 3\ ;\ 5\ ;\ 7\ ;\ 9\ ;\ 11\ ;\ 13\ ;\ 15\}.$$

9 $n = 210n'$ et $420 = 210 \times 2$.
Or, n' et 2 sont premier entre eux ; donc n' est impair, soit :

$$n' = 2k + 1 \in \mathbb{N} \quad \text{et} \quad n = 420k + 210.$$

10 **1.** $a - 2 \equiv 0 \pmod{84}$ et $a - 2 \equiv 0 \pmod{60}$; 84 et 60 divisent $a - 2$; donc $a - 2$ est divisible par le PGCD de 84 et 60.

2. PGCD$(84\ ;\ 60) = 12$.

11 PGCD$(a\ ;\ b) = 15$, donc :
PGCD$(255\,m \cap 180) = 15\,m$ et PGCD$(17\,m \cap 12) = m$.
D'où $m \in \{1\ ;\ 2\ ;\ 3\ ;\ 4\ ;\ 6\ ;\ 12\}$.

12

$$\begin{cases} a + b = 112 \\ \text{PGCD}(a;b) = 14 \end{cases} \Leftrightarrow \begin{cases} a = 14a' \\ b = 14b' \end{cases} \Leftrightarrow \begin{cases} a' + b' = 8 \\ \text{PGCD}(a';b') = 1 \end{cases}$$

Donc $(a' = 1\ ;\ b' = 7)$; $(a' = 3\ ;\ b' = 5)$
$(a' = 5\ ;\ b' = 3)$; $(a' = 7\ ;\ b' = 1)$
Donc, les couples solutions sont :

$$(14\ ;\ 98)\ ;\ (42\ ;\ 70)\ ;\ (98\ ;\ 14)\ ;\ (70\ ;\ 42).$$

13 $a = 2n^2$ et $b = n(2n + 1)$.
Or, $2n$ et $2n + 1$ sont premiers entre eux car $(2n + 1) - 2n = 1$.
Il en résulte que PGCD$(a\ ;\ b) = n$.

14 **1.** Tout diviseur d de n et $n^2 - 1$ divise $n \times n - (n^2 - 1) = 1$.
Donc n et $n^2 - 1$ sont premiers entre eux.

2. $a = n^3 + n = n(n^2 + 1)$ et $b = n^4 - 1 = (n^2 - 1)(n^2 + 1)$
Or, n et $n^2 - 1$ sont premiers entre eux.
Donc, PGCD$(n^3 + n\ ;\ n^4 - 1) = n^2 + 1$.

15 **1.** $a = 18a'$ et $b = 18b'$.
PGCD$(a'\ ;\ b') = 1$ et $18^2a'b' = 7\,776$; d'où $a'b' = 24$.
D'où le tableau :

a'	b'	a	b
1	24	18	432
3	8	54	144

Les couples solutions sont $(18\ ;\ 432)$ et $(54\ ;\ 144)$.

2. $a = 8a'$ et $b = 8b'$.
PGCD$(a'\ ;\ b') = 1$ et $b'^2 - a'^2 = 85 = (b' - a')(b' + a')$.

Donc $\begin{cases} b' + a' = 85 \\ b' - a' = 1 \end{cases}$ ou $\begin{cases} b' + a' = 17 \\ b' - a' = 5 \end{cases}$.

Soit $(a'\ ;\ b') = (42\ ;\ 43)$ ou $(a'\ ;\ b') = (6\ ;\ 11)$.
Donc $(a\ ;\ b) = (336\ ;\ 344)$ ou $(a\ ;\ b) = (48\ ;\ 88)$.

Le théorème de Bézout (page 48)

RÉSOLUTION DE PROBLÈMES

Problème 3

1. Si $11u \equiv 1 \pmod{26}$, $z \equiv z \pmod{26}$ donc :

$$11uz \equiv z \pmod{26} \quad \text{soit} \quad x \equiv zu \pmod{26}.$$

2. 11 et 26 sont premiers entre eux ; donc, il existe u et v tels que : $11u + 26v = 1$.

3. Avec $a = 11$ et $b = 26$, on a :
$26 = 2 \times 11 + 4$, soit $4 = b - 2a$;
$11 = 2 \times 4 + 3$, soit $3 = a - 2b + 4a = 5a - 2b$;
$4 = 3 + 1$, soit $1 = b - 2a - 5a + 2b = 3b - 7a$;
soit $11 \times (-7) + 26 \times 3 = 1$.
Donc $(u\,;\,v) = (7\,;\,3)$ convient.

a) $u \equiv -7 \pmod{26}$ soit $u = -7 + 26k$ ou encore $u \equiv 19 \pmod{26}$.
Or $x \equiv uz \pmod{26}$ donc $x \equiv 19(y - 8) \pmod{26}$.
Soit $x \equiv 19y - 152 \pmod{26}$.
Or $-152 \equiv 4 \pmod{26}$ d'où $x \equiv 19y + 4 \pmod{26}$.

b) La lettre du message YGMAXEGGZ se décode ainsi :
$y = 24$ et $x \equiv 460 \pmod{26}$ ou $x \equiv 18 \pmod{26}$ donc Y $\to$ S.
De même G $\to$ 0, car si $y = 6$, $x \equiv 14 \pmod{26}$ et G $\to$ 0, etc. ; le message décodé est :

SOYEZ COOL !

Problème 4

A **1.** Voir ci-après.
Avec $a = 17$ et $b = 10$, $u = 3$ et $v = -5$, soit :

$$17 \times \mathbf{3} - 10 \times \mathbf{5} = 1.$$

2. a) $43 \times \mathbf{23} - 38 \times \mathbf{26} = 1$.

b) $2\,012 \times \mathbf{114} - 347 \times \mathbf{661} = 1$.

3. Si les nombres saisis a et b ne sont pas premiers entre eux, le reste r n'est jamais égal à 1.
L'algorithme s'arrête en raison du dépassement de la capacité autorisée pour les boucles.

```
VARIABLES
  a EST_DU_TYPE NOMBRE
  b EST_DU_TYPE NOMBRE
  r EST_DU_TYPE NOMBRE
  u EST_DU_TYPE NOMBRE
  v EST_DU_TYPE NOMBRE
  m EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
  LIRE a
  LIRE b
  r PREND_LA_VALEUR 0
  u PREND_LA_VALEUR 1
  TANT_QUE (r!=1) FAIRE
    DEBUT_TANT_QUE
    m PREND_LA_VALEUR a*u
    r PREND_LA_VALEUR m%b
    u PREND_LA_VALEUR u+1
    FIN_TANT_QUE
  u PREND_LA_VALEUR u-1
  v PREND_LA_VALEUR (1-m)/b
  AFFICHER "u="
  AFFICHER u
  AFFICHER "v="
  AFFICHER v
FIN_ALGORITHME
```

Résultats

```
***Algorithme lancé***
u=3
```

B **1.** Les multiples successifs de a apparaissent dans la colonne B et les restes de la division euclidienne de au par b dans la colonne C.

2. En recopiant vers le bas, on obtient d'autres coefficients :
$\mathbf{13} \times 17 - \mathbf{22} \times 10 = 1$,
$\mathbf{23} \times 17 - \mathbf{39} \times 10 = 1$,
$33 \times 17 - 56 \times 10 = 1$, …

3. Si les nombres saisis a et b ne sont pas premiers entre eux, r ne prend jamais la valeur 1 et la colonne D reste vide.

EXERCICES

Application (page 52)

16 $2b - 3a = 6n + 4 - 6n - 3 = 1$.
Donc, d'après le théorème de Bézout, a et b sont premiers entre eux.

17 $9a - 2b = 18k + 9 - 18k - 8 = 1$.
Donc a et b sont premiers entre eux.

18 $(n^2 + 1)^2 = n^4 + 2n^2 + 1 = n(n^3 + 2n) + 1$, d'où :

$$(n^2 + 1)(n^2 + 1) - (n^3 + 2n)n = 1.$$

Donc, d'après le théorème de Bézout, $(n^2 + 1)$ et $(n^3 + 2n)$ sont premiers entre eux.

19 $a^2 + ab - b^2 - 1 = 0$, d'où $a \times a + b(a - b) = 1$.
Donc, a et b sont premiers entre eux.

20 Par hypothèse, il existe u et v tels que :

$$au + bv = 1.$$

Donc $(au + bv)^2 = 1$, soit :

$$a^2u^2 + 2abuv + b^2v^2 = 1.$$

D'où :

$$a(au^2 + 2buv) + b^2v^2 = 1.$$

Donc, d'après le théorème de Bézout, a et b^2 sont premiers entre eux.

21 **1.** a est premier avec b donc $au + bv = 1$.
Si a est premier avec b^n alors $au' + b^n v' = 1$.
Donc $(au' + b^n v')(au + bv) = 1$, soit :

$$a^2uu' + abu'v + b^n av'u + b^{n+1} v'v = 1.$$

D'où $a(auu' + bu'v + b^n v'u) + b^{n+1} vv' = 1$.
Donc a est premier avec b^{n+1}.
Ainsi, pour tout n de $\mathbb{N}^*$, a et b^n sont premiers entre eux.
2. a est premier avec b^n (*cf.* **1.**). Si a^p est premier avec b^n, démontrons que a^{p+1} est premier avec b^n.

$$a^p u + b^n v = 1 \text{ et } au' + b^n v' = 1 ;$$

donc $a^{p+1}(uu') + b^n(a^p uv' + avu' + b^n vv') = 1$.
Donc a^{p+1} est premier avec b^n.
Ainsi, pour tout $p \in \mathbb{N}^*$, a^p est premier avec b^n.
3. a et b sont deux entiers naturels non nuls tels que a est premier avec b. Alors pour tous entiers p et n, a^p est premier.

22 **1.** Par définition, si Δ est le PGCD$(bc - a ; b)$, alors il existe deux entiers relatifs u et v tels que :

$$(bc - a)u + bv = \Delta.$$

2. D'où $a(-u) + b(uc + v) = \Delta$.
Donc Δ est le PGCD de a et b.

23 **1.** On note Δ, le PGCD$(n - p^2 ; p)$.
Donc $(n - p^2)u + pv = \Delta$. Soit $nu + p(-pu + v) = \Delta$.
Donc Δ et le PGCD$(n ; p)$.
2. PGCD(10 829 ; 104) = PGCD(10 829 – $(104)^2$; 104).
Soit PGCD(13 ; 104) = 8.

24 On note Δ, le PGCD$(a ; 3a + b)$.
Donc $au + (3a + b)v = \Delta$.
Soit $a(u + 3v) + bv = 1$. Donc Δ = PGCD$(a ; b)$.

25 Par hypothèse, $au + bv = 1$.
Si Δ est le PGCD$(a + b ; ab)$ alors :

$$(a + b)\alpha + ab\beta = \Delta.$$

Or, a et b sont premiers entre eux donc $\Delta = 1$.

SÉQUENCE 3 Le théorème de Gauss (page 54)

RÉSOLUTION DE PROBLÈMES

Problème 5

A **1.** $a \equiv a'$ (mod 26) et $b \equiv b'$ (mod 26), alors :

$$ax + b \equiv a'x + b' \text{ (mod 26)}.$$

2. a) On a 25 choix pour a et 25 choix pour b ; donc 625 clés de codage.

mot à coder	P	A	L	A	C	E
nombre associé à la lettre	15	0	11	0	2	4
code : $y = 4x + 3$	63	3	47	3	11	19
$ax + b \equiv \ldots$ (mod 26)	11	3	21	3	11	19
mot codé	L	D	V	D	L	T

Si on cherche à déchiffrer le message, L correspond à 2 lettres différentes à savoir P et C.

B **1.** Pour les propositions, l'une est la transposée de l'autre. Elles sont donc équivalentes.

2. et **3.** Si $a(x - x') \equiv 0$ (mod 26), alors $a(x - x') = 26k$ ($k \in \mathbb{Z}$).
Si a est premier avec 26, comme 26 divise $a(x - x')$, alors 26 divise $x - x'$; donc $x \equiv x'$ (mod 26).
Or $0 \leqslant x \leqslant 25$ et $0 \leqslant x' \leqslant 25$, donc $x = x'$.

4. Ainsi, pour qu'un chiffrement soit utilisable, il suffit que a soit premier avec 26. Donc a doit être différent de 1 et de 13 et être impair.
Il y a donc 11 valeurs pour a, soit 265 clés possibles.
Le nombre possible de clés est petit. Ainsi, il est très facile de « casser » ce code : un algorithme mettant en œuvre les 265 clés possibles permettra rapidement de déchiffrer le message.

Problème 6

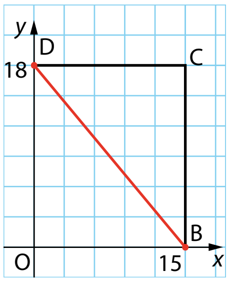
1. a) Avec les 6 jours de décalage, $105u - 81v = 6$, soit $35u - 27v = 2$.
2. a) $35 \equiv 8$ (mod 27) ; donc, si $35u - 27v = 2$, $8u \equiv 2$ (mod 27) et $u_0 = 7$.
b) $35 \times 7 - 2 = 27v_0$, soit $27v_0 = 243$ et $v_0 = 9$.
3. a) $35(u - 7) = 27(v - 9) \Leftrightarrow 35u - 27v = 35 \times 7 - 9 \times 27$
$= 2$.
b) 27 divise $35(u - 7)$; or 27 est premier avec 35 ; donc 27 divise $u - 7$. Il en résulte que $u = 27k + 7$ et $v = 35k + 9$.
c) Si $k = 0$, $u = 7$ et $v = 9$, d'où $105 \times 7 = 735$ jours, soit k est le 19 juillet 2014.
d) Pour $k = 1$, $u = 34$ soit $105 \times 34 = 3\,570$ jours…

EXERCICES Application (page 57)

26 **a)** $11x = 6y$. 6 divise $11x$ et 6 est premier avec 11. Donc, d'après le théorème de Gauss, 6 divise x.
Ainsi, $x = 6k$ et $y = 11k$ ($k \in \mathbb{N}$).
$x \in \{0 ; 6 ; 12 ; 18 ; 24\}$ et $y \in \{0 ; 11 ; 22 ; 33 ; 44\}$.
On obtient les couples :
$(0 ; 0) ; (6 ; 11) ; (12 ; 22) ; (18 ; 33) ; (24 ; 44)$.
b) Pour la même raison que pour **a)**, $x = 7k$ et $y = 3k$.
Donc $x = 0$ ou 7 ou 14. On obtient les couples :
$(0 ; 0) ; (7 ; 3) ; (14 ; 6)$.

27 $4x = 3(y - 4)$.
3 divise $4x$ et 3 est premier avec 4 ; donc 3 divise x.
D'où $x = 3k$ et $y = 4 + 4k$ ($k \in \mathbb{N}$).

28 $\overrightarrow{BD}(-15 ; 18)$, donc $\vec{u}(-5 ; 6)$ est un vecteur directeur de (BD).
(BD) a une équation de la forme $6x + 5y + d = 0$.
B $\in$ (BD) donc $90 + d = 0$, d'où $d = -90$. Donc (BD) a pour équation :
$$6x + 5y - 90 = 0,$$



d'où $6x = 5(-y + 18)$.
5 divise $6x$ et 5 est premier avec 6 ; donc 5 divise x et $x = 5k$; $y = -6k + 18$.
$0 \leqslant x \leqslant 15$ donc $0 \leqslant k \leqslant 3$.
Si $k = 0$, $x = 0$ et $y = 18$.
Si $k = 1$, $x = 5$ et $y = 12$.
Si $k = 2$, $x = 10$ et $y = 6$.
Si $k = 3$, $x = 15$ et $y = 0$.

29 **1.** 7 est premier avec 3 et 7 divise $3(x - 4)$; donc, d'après le théorème de Gauss, 7 divise $(x - 4)$.
2. On a donc :
$x - 4$ (mod 7) avec $x \equiv 4$ (mod 7) et $x = 7k + 4$ ($k \in \mathbb{Z}$).

30 $a = n(n + 1)(n + 5)$.
n et $n + 1$ sont deux entiers consécutifs. Donc 2 divise a.
De plus, $n + 5 \equiv n + 2$ (mod 3).
Or $n(n+1)(n + 2)$ est le produit de trois entiers consécutifs ; donc divisible par 3. Or 2 et 3 sont premiers entre eux ; donc a est divisible par 6.

31 Restes de la division de $a = n(n + 1)(n + 2)(n + 3)$ par 8

$n \equiv$	0	1	2	3	4	5	6	7
$n + 1$	1	2	3	4	5	6	7	0
$n + 2$	2	3	4	5	6	7	0	1
$n + 3$	3	4	5	6	7	0	1	2
a	0	0	0	0	0	0	0	0

Donc a est divisible par 8. De plus $n(n + 1)(n + 2)$, produit de trois entiers consécutifs, est divisible par 3. Il en résulte que a est divisible par 24 car 8 et 3 sont premiers entre eux.

32 On pose : $A = 2n(2n + 2)(2n + 4)$
$A = 8n(n + 1)(n + 2)$.
On sait que $B = n(n + 1)(n + 2)$ est divisible par 6 (*cf.* **30**) donc 8B est divisible par 48.

33 On pose $A = p(p + 1)(p + 2)(p + 3)(p + 4)(p + 5)$.
D'après l'exercice **31** $p(p + 1)(p + 2)(p + 3)$ est divisible par 24. Il reste à démontrer que A est divisible par 5. On construit le tableau des restes dans la congruence modulo 5 ci-dessous.

$p \equiv$	0	1	2	3	4
$p + 1 \equiv$	1	2	3	4	0
$p + 2 \equiv$	2	3	4	0	1
$p + 3 \equiv$	3	4	0	1	2
$p + 4 \equiv$	4	0	1	2	3
$p + 5 \equiv$	0	1	2	3	4
$A \equiv$	0	0	0	0	0

Donc, A est divisible par 24 et 5 qui sont premiers entre eux donc divisibles par 120.

34 On pose $A = n(n^2 + 2)(n^2 + 7)$.
• Dans la congruence modulo 3, on construit le tableau ci-dessous :

$n \equiv$	0	1	2
$n^2 \equiv$	0	1	1
$n^2 + 2 \equiv$	2	0	0
$n(n^2 + 2) \equiv$	0	0	0

Donc $A \equiv 0$ (modulo 3).
• Dans la congruence modulo 8, on construit le tableau ci-dessous :

$n \equiv$	0	1	2	3	4	5	6	7
$n^2 \equiv$	0	1	4	1	0	1	4	1
$n^2 + 2 \equiv$	2	3	6	3	2	3	6	3
$n^2 + 7 \equiv$	7	0	3	0	7	0	3	0
$A \equiv$	0	0	4	0	0	0	4	0

Donc, si n est impair : $A \equiv 0$ (mod 8).
Donc, si n est impair : $A \equiv 0$ (mod 24).

35 **1.** Si x est congru à 0, 1 ou 2 modulo 3, alors x^2 est congru à 0 ou 1. D'ou le tableau des restes de $a^2 + b^2$ modulo 3 :

b^2 \ a^2	0	1
0	0	1
1	1	2

Ainsi $a^2 + b^2$ est congru à 0, 1, ou 2 (mod 3).
2. $a^2 + b^2 \equiv 0$ (mod 3) $\Leftrightarrow a^2 \equiv 0$ (mod 3) et $b^2 \equiv 0$ (mod 3).
Donc $a = 3k$ et $b = 3k'$ donc a et b sont divisibles par 3.
Conclusion : si a et b sont premiers entre eux, $a^2 + b^2$ est congru à 1 ou 2 modulo 3.

EXERCICES Activités de recherche (page 60)

40 **Trouver un PGCD**

• Les outils

– La divisibilité.
– Définition du PGCD.
– Propriétés du PGCD.

• Les objectifs

– Savoir utiliser les propriétés du PGCD.
– Savoir utiliser x divise y et y divise x pour établir que $x = y$.

1. Tout diviseur Δ de A et B est un diviseur de leur PGCD δ ; donc $\Delta \leqslant \delta$.

2. Si δ divise a et b, δ divise toute combinaison linéaire de a et b ; donc A et B. Ainsi $\Delta \geqslant \delta$ et $\Delta = \delta$.

3. $\begin{cases} ap+qb=\mathrm{A} \\ ra+sb=\mathrm{B} \end{cases} \Leftrightarrow \begin{cases} -r(ap+qb)+p(ra+sb)=\mathrm{B}p-\mathrm{A}r \\ s(ap+qb)-q(ra+sb)=s\mathrm{A}-q\mathrm{B} \end{cases}$

Donc $\begin{cases} (ps-qr)b=\mathrm{B}p-\mathrm{A}r \\ (sq-qr)a=s\mathrm{A}-q\mathrm{B} \end{cases}$

Or $ps - qr = 1$, donc :

$$b = \mathrm{B}p - \mathrm{A}r \text{ et } a = s\mathrm{A} - q\mathrm{B}.$$

Si δ divise A et B, alors δ divise a et b.
Ainsi, $\delta \leqslant \Delta$ et $\delta \geqslant \Delta$; donc $\Delta = \delta$.

41 **Le théorème des restes chinois**

• Les outils

– Le théorème de Bézout.
– Le théorème de Gauss.

• Les objectifs

– Savoir établir une équivalence.
– Savoir reconnaître et appliquer les théorèmes de Bézout et Gauss.

1. a) $\begin{cases} n\equiv 5 \pmod 7 \\ n\equiv 4 \pmod{11} \end{cases} \Leftrightarrow \left.\begin{cases} n=7p+5 \\ n=11q+4 \end{cases}\right\}(S)$

b) $(S) \Leftrightarrow \begin{cases} n=7p+5 \\ 7p+5=11q+4 \end{cases} \Leftrightarrow (S')\begin{cases} n=7p+5 \\ 11q-7p=1 \end{cases}$

c) D'après le théorème de Bézout, 11 et 7 sont premiers entre eux. Donc, il existe p et q tels que $11q - 7p = 1$.

d) $11(q - 2) = 7(p - 3) \Leftrightarrow 11q - 7p = 1$.

e) 7 divise $11(q - 2)$ et 7 est premier avec 11. Donc 7 divise $q - 2$; d'où $q - 2 = 7k$, soit $q = 7k + 2$.
De plus, $p = 11k + 3$ ($k \in \mathbb{N}$) ; donc :

$$n = 7(11k + 3) + 5 = 77k + 26.$$

42 **Trouver des entiers connaissant leur somme et leur PGCD**

• Les outils

– Propriétés du PGCD.
– Nombres premiers entre eux.

• Les objectifs

– Savoir utiliser la disjonction des cas.
– Savoir utiliser les propriétés du PGCD.

$a + b = 40$ et PGCD$(a ; b) = 5$ ($a \in \mathbb{Z}$) ($b \in \mathbb{Z}$).

1. a) $a = 5a'$ et $b = 5b'$.
$5(a' + b') = 40$; donc $a' + b' = 8$ et PGCD$(a' ; b') = 1$.
Si a' et b' étaient pairs, ils ne seraient pas premiers entre eux. Si l'un est pair et l'autre impair, la somme est impaire donc différente de 8. Il en résulte que a' et b' sont impairs.

2. $a' = 2k + 1$; donc $b' = 8 - a' = 7 - 2k$.

3. a) $a' + b' = 8$, donc tout diviseur de a' et b' divise leur somme $a' + b'$ donc divise 8.
b) a' et b' étant impairs, ils ne peuvent avoir de diviseurs pairs.
c) Il résulte que « 1 » est le seul diviseur commun ; donc PGCD$(a' ; b') = 1$.
On conclut que :

$$a = 10k + 5 \text{ et } b = 35 - 10k \ (k \in \mathbb{Z}).$$

43 **Narration de recherche**

$3x - 5y = 6$ (1).
Le couple $(x ; y) = (12 ; 6)$ est solution de (1) ; donc :

$$\begin{cases} 3x-5y=6 \\ 3\times 12-5\times 6=6 \end{cases} \Leftrightarrow 3(x-12)=5(y-6)$$

Or, 5 est premier avec 3 et divise $3(x - 12)$; donc 5 divise $(x - 12)$. Il en résulte que :

$$x = 5k + 12 \text{ et } y = 3k + 6.$$

Or, $y \equiv x^2 \pmod 5$; donc :

$$3k + 6 \equiv 25k^2 + 120k + 144 \pmod 5 ;$$

soit $25k^2 + 117k + 138 \equiv 0 \pmod 5$.
Donc $2k + 3 \equiv 0 \pmod 5$ ou $2k \equiv 2 \pmod 5$.

$k \equiv$	0	1	2	3	4
$2k \equiv$	0	2	4	1	3

donc $k \equiv 1 \pmod 5$ et $k = 5p + 1$.
Il en résulte que $x = 25p + 17$ et $y = 15p + 9$ ($p \in \mathbb{N}$).
On vérifie simplement que :

$$3x - 5y = 6 \text{ et } y = x^2 \pmod 5.$$

44 **Narration de recherche**

$b = aq$; $c = aq^2$; $d = aq^3$;

donc :

$$10a^2 = aq(q^2 - 1)\ (q \neq 0)\ \ (a \neq 0)$$
$$10a = q(q^2 - 1)\ (2)$$

q divise $10a$ et q est premier avec a.

Donc q divise 10 et $q \in \{1 ; 2 ; 5 ; 10\}$.

$q = 1$ ne convient pas car $a \neq 0$;

$q = 2$ ne convient pas car $5a = 3$; a n'est pas entier.

Si $q = 5$, $2a = 24$, d'où $a = 12$;

si $q = 10$, $a = 99$.

En conclusion :

$$a = 12 ; b = 60 ; c = 300 ; d = 1\,500$$

ou $a = 99$; $b = 990$; $c = 9\,900$; $d = 99\,000$.

45 **TD – Le plus petit commun multiple de deux entiers naturels strictement positifs**

A. 1. $\Delta = \text{PGCD}(a ; b) = 18$; $a = 18 \times 2$ et $b = 18 \times 3$; donc $a' = 2$ et $b' = 3$.

2. $1\,944 = 36 \times 54$; donc 1 944 est un multiple commun à 36 et 54.

$504 = 36 \times 14$ et 54 ne divise pas 504.

Donc 504 n'est pas un multiple commun.

3. $108 = 2 \times 54 = 3 \times 36$.

B. 1. a) $\Delta = \Delta a'$; $b = \Delta b'$; $\text{PGCD}(a' ; b') = 1$.

$M = pa = pa'\Delta = qb'\Delta$ donc $pa' = qb'$.

b) a' divise qb' et a' premier avec b'. Donc a' divise q, soit $q = ka'$ et $pa' = ka'b'$; soit $p = kb'$.

2. a) $M = k\Delta a'b'$ ($k \in \mathbb{N}^*$).

b) $k = 1$ est la plus petite valeur ; donc le PPCM est $\Delta a'b'$; soit $m\Delta = \Delta a'\Delta b' = ab$.

C. 1. $\text{PPCM}(a ; b) - 9$; $\text{PGCD}(a ; b) = 13$; $a < b$

$m - 9\Delta = 13 \Leftrightarrow \Delta a'b' - 9\Delta = 13$, soit $\Delta(a'b' - 9) = 13$.

2. Δ divise 13, donc $\Delta = 1$, ou $\Delta = 13$.

Si $\Delta = 1$, $a'b' = 22$.

Si $\Delta = 13$, $a'b' = 10$.

• $\Delta = 1$

a'	b'	a	b
1	22	1	22
2	11	2	11

• $\Delta = 13$

a'	b'	a	b
1	10	13	130
2	5	26	65

46 **TD – Résoudre une équation diophantienne**

A. 1. $\text{PGCD}(39 ; 27) = 3$ donc $(1) \Leftrightarrow 13x + 9y = 6$.

2. a) 13 et 9 sont premiers entre eux.

Donc, il existe u et v tels que $13x + 9y = 1$.

b) On remarque $13(-2) + 9(3) = 1$.

D'où $13(-12) + 9(18) = 6$.

Donc $(-12 ; 18)$ est une solution particulière.

3. a) $13(x + 12) = 9(18 - y)$.

9 divise $13(x + 12)$ et 9 est premier avec 13.

Donc 9 divise $x + 12$; d'où $x = 9k - 12$ et $y = 18 - 13k$.

b) *Vérification :* $13(9k - 12) + 9(18 - 13k) = -156 + 162 = 6$.

B. 1. $7x + 6y = 3$ et $7 \times 3 + 6(-3) = 3$.

Donc $7(x - 3) + 6(y + 3) = 0$, d'où $7(3 - x) = 6(y + 3)$.

6 divise $7(3 - x)$ et 6 est premier avec 7 ; donc 6 divise $3 - x$, soit $3 - x = 6k$.

Donc $x = 3 - 6k$ et $y = 7k - 3$.

Vérification : $7(3 - 6k) + 6(7k - 3) = 3$.

2. a) $3x - y = 8$, $3 \times 3 - 1 = 8$; donc $3(x - 3) - (y - 1) = 0$.

3 divise $y - 1$; donc $y = 3k + 1$ et $x = k + 3$.

Vérification : $3k + 9 - 3k - 1 = 8$.

b) $\text{PGCD}(3 ; 6) = 3$; or 3 ne divise pas 5. Donc l'équation n'a pas de solution.

c) $4x + 6y = 22 \Leftrightarrow 2x + 3y = 11$

$2(-2) + 3 \times 5 = 11$; donc $2(x + 2) + 3(y - 5) = 0$;

soit $2(x + 2) = 3(5 - y)$.

Donc $x = 3k + 2$ et $y = 5 - 2k$.

Vérification : $2(3k - 2) + 3(5 - 2k) = 11$.

47 **TD – Des coïncidences ?**

A. 1. a) L'origine des temps est minuit. Les éclairs rouges apparaissent donc à $8 + 24r$ ($r \in \mathbb{N}$).

b) L'éclair vert apparaît donc à $20 + 28v$ ($v \in \mathbb{N}$).

c) Il y a 149 éclairs rouge et 127 éclairs verts.

d) La première coïncidence a lieu à minuit, une minute et 44 secondes. Il y a 21 coïncidences

B. 1. La prochaine apparition simultanée a lieu à :

$8 + 24r = 20 + 28v$ soit $24r - 28v = 12$ ou $6r - 7v = 3$.

2. 6 et 7 sont premiers entre eux ; donc, il existe des solutions.

3. $6r - 7v = 3$, d'où $6(-3) - 7(-3) = 3$;

donc $6(r + 3) - 7(v + 3) = 0$, soit $6(r + 3) = 7(v + 3)$.

7 divise $r + 3$ car 7 est premier avec 6 ;

donc $r = 7k - 3$ et $v = 6k - 3$, le $k \in \mathbb{N}^*$.

4. Si $k = 1$, $r = 4$ et $v = 3$.

Donc, la prochaine apparition est à :

$$8 + 24 \times 4 = 8 + 96 = 104 \text{ s.}$$

Soit, à minuit, 1 minute 44 secondes.

Avant 1 h du matin, il y a 21 coïncidences ; la dernière ayant lieu à minuit 55 minutes 56 secondes.

Car $\quad 0 \leqslant 8 + 24(7k - 3) \leqslant 3\,600$

$$64 \leqslant 168k \leqslant 3\,664$$
$$1 \leqslant k \leqslant 21\ \ (k \in \mathbb{N})$$

Soit 21 valeurs de k.

C. 1. À l'aide du tableur, on ne trouve pas de solution.

On a donc $7 + 24r = 20 + 28v$, d'où $24r - 28v = 13$.

Or, $\text{PGCD}(24 ; 28) = 4$ ne divise pas 13. Il n'y a donc pas de solution.

EXERCICES Entraînement (page 65)

DE TÊTE

48 Faux ; il peut être égal à 1 ou à 3.
Exemple. $x = -3$ et $y = 6$.

49 PGCD$(a\,;b) = 42$.

50 $a = 4a'$; $b = 4b'$; $a' + b' = 12$.
D'où $a = 4$ et $b = 44$.

51 Non, car 11 ne divise pas 100.

52 7 divise x ; donc $x = 7$ ou 14.
D'où (7 ; 3) et (14 ; 6).

53 $2n + 1 - 2(n) = 1$; PGCD$(2n + 1\,;n) = 1$.

54 $b \in \{23\,;25\,;29\}$.

PGCD DE DEUX NOMBRES ENTIERS

55 $2\,173 = 1\,961 + 212$, d'où $1\,961 = 9 \times 212 + 53$, soit $212 = 4 \times 53$.
Donc, PGCD$(2\,173\,;1\,961) = 53$.
Ces nombres ne sont pas premiers entre eux.

56 **a)** 63 et 100 sont premiers entre eux.
Donc PGCD$(a\,;b) = 24$.
b) Même raison qu'au **a)**.
PGCD$(a\,;b) = 26$.

57 $4\,840 \equiv 4 \pmod d$ et $4\,190 \equiv 5 \pmod d$.
Donc, d divise 4 836 et 4 185.
Or, PGCD(4 836 ; 4 185) $= 93 = 3 \times 31$.
Donc $d = 93$ ou 31, car $d > 5$.

58 $a = 2b + r_1$ donc $r_3 = 13$.
$b = r_1 + r_2$ donc $r_2 = 39$.
$r_1 = 2\,r_2 + r_3$ donc $r_1 = 91$.
$r_2 = 3 \times r_3$ donc $b = 130$ et $a = 351$.

59 **1.** Tout diviseur de a et $b - a$ divise leur somme $a + (b - a) = b$.
Donc, tout diviseur de a et $b - a$ divise a et b et réciproquement.
Donc :
PGCD$(a\,;b) =$
PGCD$(a\,;b - a)$.
2. a) Avec AlgoBox : voir ci-contre.

```
VARIABLES
  a EST_DU_TYPE NOMBRE
  b EST_DU_TYPE NOMBRE
  c EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
  LIRE a
  LIRE b
  TANT_QUE (a!=b) FAIRE
    DEBUT_TANT_QUE
    SI (a>b) ALORS
      DEBUT_SI
      c PREND_LA_VALEUR a
      a PREND_LA_VALEUR b
      b PREND_LA_VALEUR c
      FIN_SI
      SINON
        DEBUT_SINON
        b PREND_LA_VALEUR b-a
        FIN_SINON
    FIN_TANT_QUE
  AFFICHER "Pgcd (a;b) = "
  AFFICHER a
FIN_ALGORITHME
```

b) PGCD$(147\,;450) =$ PGCD$(147\,;303)$
$=$ PGCD$(147\,;156)$
$=$ PGCD$(147\,;9)$
$= 3$PGCD$(49\,;3)$.
D'où PGCD$(147\,;450) = 3$.

60 Si d divise b et $a - 2b$, d divise $2b + a - 2b = 0$; donc d divise a et b.
Réciproquement, si d divise a et b, d divise toute combinaison linéaire ; soit $a - 2b$. Donc $\mathcal{D}(a\,;b) = \mathcal{D}(b\,;a - 2b)$.

61 **1.** Si d divise a et b, d divise $3(2n + 5) - 2(3n + 4)$; donc d divise 7.
2. $2n + 5 \equiv 0 \pmod 7 \Leftrightarrow 2n \equiv 2 \pmod 7$.

$n \equiv$	0	1	2	3	4	5	6
$2n \equiv$	0	2	4	6	1	3	5

Donc $n \equiv 1 \pmod 7$ et $3n + 4 \equiv 0 \pmod 7 \Leftrightarrow 3n \equiv 3 \pmod 7$ donc $n \equiv 1 \pmod 7$.
a et b sont divisibles par 7 si, et seulement si, $n \equiv 1 \pmod 7$.
Si $n \neq 7k + 1$, alors PGCD$(a\,;b) = 1$.

62 Si Δ divise $n + 1$ et $n + 3$, Δ divise $(n + 3) - (n + 1) = 2$.
Donc le PGCD possible est 1 ou 2.
Si n est impair, PGCD$(a\,;b) = 2$;
et si n est pair, PGCD$(a\,;b) = 1$.

63 *Corrigé sur le site élève.*

64 $x = 17x'$ et $y = 17y'$; PGCD$(x'\,;y') = 1$.
Donc $17^2x'y' = 1\,734$, soit $x'y' = 6$.

x'	y'	x	y
1	6	17	102
2	3	34	51

65 *Corrigé sur le site élève.*

66 **1.** Tout diviseur de n et $n^2 - 1$ divise :
$$n(n) - (n^2 - 1) = 1\ ;$$
donc PGCD$(n\,;n^2 - 1) = 1$.
2. $a = n(n + 1)$ et $b = (n + 1)(n^2 - 1)$.
Comme n et $n^2 - 1$ sont premiers entre eux, on a :
$$\text{PGCD}(a\,;b) = n + 1.$$

67 **1.** $(n - 1)(n - 2) + 4 = n^2 - 3n + 6$.
2. $a - (n - 2)b = 4$; donc tout diviseur de a et b divise 4.
Ainsi PGCD$(a\,;b) =$ PGCD$(n - 1\,;4)$.
3. a) Les PGCD possibles sont 1, 2 ou 4.
b) Si $n = 4k$, $n - 1 = 4k - 1$ et $4(k) - (4k - 1) = 1$; donc PGCD$(a\,;b) = 1$.
Si $n = 4k + 1$, $n - 1 = 4k$ et PGCD$(a\,;b) = 4$.
Si $n = 4k + 2$, $n - 1 = 4k + 1$ et PGCD$(a\,;b) = 1$.
Si $n = 4k + 3$, $n - 1 = 2(2k + 1)$;
donc PGCD$(n - 1\,;n) = 2\,$PGCD$(2k + 1\,;2)$.
Or PGCD$(2k + 1\,;2) = 1$; donc PGCD$(a\,;b) = 2$.

THÉOREME DE BÉZOUT

68 (1 ; 12) ; (5 ; 7) ; (7 ; 5) ; (12 ; 1).

69 **1.** $9b - 7a = 63n + 36 - 63n - 35 = 1$.
2. D'après le théorème de Bézout, PGCD$(a\ ;\ b) = 1$.

70 **1.** $(n^2 + 1)^2 = n^4 + 2n^2 + 1 = n(n^3 + 2n) + 1$.
2. $(n^2 + 1)(n^2 + 1) - n((n^3 + 2n) = 1$.
Donc, d'après le théorème de Bézout :
$$\text{PGCD}(n^2 + 1\ ;\ n^3 + 2n) = 1.$$

71 *Corrigé sur le site élève.*

72 $a - 2nb = 1$.
Donc, a et b sont premiers entre eux.

73 **1.** $a = 2x + y$ et $b = 5x + 2y$.
Donc $x = b - 2a$ et $y = 5a - 2b$.
Si d divise a et b, alors d divise x et y.
Donc, tout diviseur de a et b est un diviseur de x et y. De même, tout diviseur de x et y divise a et b. Donc, si PGCD$(x\ ;\ y) = 1$ alors PGCD$(a\ ;\ b) = 1$.
2. $a = 3a'$; $b = 3b'$ et PGCD$(a'\ ;\ b') = 1$.
Donc $9(2a' + b')(5a' + 2b') = 1\ 620$
$(2a' + b')(5a' + 2b') = 180$.
D'après **1.** PGCD$(2a' + b'\ ;\ 5a' + 2b') = 1$, d'où :
$$180 = 9 \times 20 = 3^2 \times 2^2 \times 5.$$
La seule solution est : $a = 6$ et $b = 15$.

74 **1. a)** $5(14n + 3) - 14(5n + 1) = 1$.
Donc, d'après le théorème de Bézout, les entiers $14n + 3$ et $5n + 1$ sont premiers entre eux.
b) Si $n = 6$:
$$\text{PGCD}(14 \times 6 + 3\ ;\ 5 \times 6 + 1) = 1$$
$$\text{PGCD}(87\ ;\ 31) = 1$$
2. $u = 5$ et $v = -14$ ont une solution particulière.

75 $8^m = 2 \times 16^n \Leftrightarrow 2^{3m} = 2^{4n+1}$; donc $3m - 4n = 1$.
D'après le théorème de Bézout, PGCD$(m\ ;\ n) = 1$.

76 Par hypothèse, $au + b^2v = 1$; soit $au + b(bv) = 1$; donc a et b sont premiers entre eux.

77 Si d divise $a - b$ et b, d divise $(a - b) + b = a$; donc d divise a et b ; d'où d divise Δ le PGCD$(a\ ;\ b)$.
De même, si d divise a et b, d divise a et $a - b$. Donc PGCD$(a\ ;\ b)$ = PGCD$(a - b\ ;\ b)$.

THÉORÈME DE GAUSS

78 **a)** 7 divise $(x - 2)$; donc $x = 7k + 2$ et $y = 5k$.
b) $57x = 10y$; donc 10 divise x soit $x = 10k$ et $y = 57k$.

79 **1.** Par hypothèse, $au + bv = 1$; donc :
$(au + bv)^3 = 1 \Leftrightarrow a(u^3a^2 + 3abuv + 3ub^3v^2) + b^3v^3 = 1$;
a et b^3 sont donc premiers entre eux.

2. a) $a^3 + a = 7b^3 \Leftrightarrow a(a + 1) = 7b^3$.
a divise $7b^3$ et a est premier avec b^3.
Donc a divise 7 ; soit $a = 1$ ou $a = 7$.
b) Si $a = 1$, $2 = 7b^3$; il n'y a pas de solution.
Si $a = 7$, $56 = 7b^3$, $b^3 = 8$; $b = 2$ et $a = 7$.

80

$n \equiv$	0	1	2	3	4	5
$n^3 \equiv$	0	1	2	3	4	5
$5n \equiv$	0	5	4	3	2	1
$n^3 + 5n \equiv$	0	0	0	0	0	0

Donc $n^3 + 5n$ est divisible par 6.

81 *Corrigé sur le site élève.*

82 $n \equiv 5 \pmod 6$; $n \equiv 5 \pmod 9$; $n \equiv 5 \pmod{12}$.
Donc $n - 5$ est divisible par 6, 9, 12.
Donc $n - 5$ est un multiple de 36.
Soit $n - 5 = 972$ et $n = 977$.

83 **1.** $x - 3 \equiv 0 \pmod 5$ et $x - 3 \equiv 0 \pmod{11}$.
Or PGCD$(5\ ;\ 11) = 1$, donc $x - 3 \equiv 0 \pmod{55}$.
2. $x = 55k + 3$ $(k \in \mathbb{Z})$.
3. $a = 55k + 3$ et $b = 55k + 58$.
Ces nombres sont premiers entre eux.

84 **1.** $5(x - 3) = 4(y - 3) \Leftrightarrow 5x - 4y = 3$.
2. 4 divise $5(x - 3)$ et 4 est premier avec 5.
Donc 4 divise $x - 3$; soit $x = 4k + 3$ et $y = 5k + 3$ $(k \in \mathbb{Z})$.

85 **1.** 5 divise $x - 3$; donc $x = 5k + 3$ et $y = 9k + 5$.
2. $9x \equiv 2 \pmod 5 \Leftrightarrow 9x - 5y = 2$; donc $x = 5k + 3$.

86 $x - 7 \equiv 0 \pmod{15}$; $x - 7 \equiv 0 \pmod{18}$; $x - 7 \equiv 0 \pmod{25}$.
$x - 7$ est un multiple de 15, 18 et 25 ; le plus petit est 450.
Ainsi, le prochain départ simultané aura lieu dans 7 h 30 minutes, soit à 14 h 30 minutes.

87 $n^2 + n + 4 \equiv 0 \pmod 3 \Leftrightarrow n \equiv 1 \pmod 3$
$n^2 + n + 4 \equiv 0 \pmod 5 \Leftrightarrow n \equiv 2 \pmod 5$.
Donc $3p + 1 = 5q + 2$, soit $3p - 5q = 1$.
$p = 2$ et $q = 1$ est une solution particulière ;
donc $3(p - 2) = 5(q - 1)$. 5 divise $p - 2$, soit :
$$p = 5k + 2 \text{ et } q = 3k + 1.$$
Donc $n = 3(5k + 2) + 1 = 15k + 7$ $(k \in \mathbb{N})$.

88 *Corrigé sur le site élève.*

FRACTIONS IRRÉDUCTIBLES

89 $a = \Delta a'$; $b = \Delta b'$; PGCD$(a'\ ;\ b') = 1$.
Donc $\dfrac{a}{b} = \dfrac{\Delta a'}{\Delta b'} = \dfrac{a'}{b'}$; donc $\dfrac{a}{b}$ est égale à la fraction irréductible $\dfrac{a'}{b'}$.

90 • $(2n+3)-2(n+1)=1$; donc $2n+3$ et $n+1$ sont premiers entre eux.

La fraction $\dfrac{2n+3}{n+1}$ est irréductible.

• $3(4n+3)-4(3n+2)=1$.

La fraction $\dfrac{4n+3}{3n+2}$ est irréductible.

91 **1. a)** $(2n+5)-2(n+2)=1$; donc $2n+5$ et $n+2$ sont premiers entre eux.

$2(n+3)-(2n+5)=1$; donc $2n+5$ et $n+2$ sont premiers entre eux.

b) $(2n+5)$ est premier avec $(n+2)(n+3)$, donc $(2n+5)$ est premier avec n^2+5n+6.

2. Il en résulte que la fraction A est une fraction irréductible.

92 *Corrigé sur le site élève.*

93 $(n+3)-(n-4)=7$; donc, tout diviseur de $(n+3)$ et $(n-4)$ divise 7.

Les diviseurs de 7 sont 1 et 7.

$n-4\equiv 0 \pmod 7$ si $n=7k+4$.

$n+3=7(k+1)$, donc PGCD$(n+3\,;\,n-4)=7$.

Pour les autres valeurs de n, le PGCD $(n+3\,;\,n-4)=1$; donc la fraction A est irréductible.

94 **1.** $a_n\dfrac{p^n}{q^n}+\ldots+a_1\dfrac{p}{q}+a_0=0$

$a_np^n+\ldots+a_1pq^{n-1}+a_0q^n=0$

$p(a_np^{n-1}+\ldots+a_1q^{n-1})=-a_0q^n$.

PGCD$(p\,;\,q^n)=1$ donc p divise a_0.

De même, $-a_np^n=q[a_{n-1}p^{n-1}+\ldots+a_0q^{n-1}]$.

PGCD$(p^n\,;\,q)=1$ donc q divise a_n.

2. a) p divise 1 et q divise 3.

Donc, les solutions possibles sont $\dfrac{1}{3}$ et $-\dfrac{1}{3}$.

On vérifie que $\dfrac{1}{3}$ convient.

b) $\dfrac{1}{3}$ vérifie l'équation :

$$3x^3-19x^2+9x-1=0.$$

$3x^3-19x^2+9x-1=(3x-1)(x^2-6x+1)$;

d'où $x^2-6x+1=0$ a pour solution :

$$x_1=3-2\sqrt{2} \quad\text{et}\quad x_2=3+2\sqrt{2}.$$

Donc $\mathcal{S}=\left\{\dfrac{1}{3}\ ;\ 3-2\sqrt{2}\ ;\ 3+2\sqrt{2}\right\}$.

RÉSOUDRE DES ÉQUATIONS DANS $\mathbb{N}$ OU $\mathbb{Z}$

95 **1.** $8x=5(20-y)$.

5 premier avec 8 divise $8x$; donc :

$$x=5k \quad\text{et}\quad y=20-8k.$$

2. Soit x hommes et y femmes. On a $8x+5y=100$; soit $8x=5(20-y)$.

Donc $x=5k$ et $y=20-8k$ $(k\in\mathbb{N}^*)$.

Or $20-8k>0$, d'où $k<\dfrac{5}{2}$ et $k>0$; donc $k\in\{1\,;\,2\}$.

Dans le groupe, il y a 5 hommes et 12 femmes ou 10 hommes et 4 femmes.

96 **1. a)** $6y\equiv 0 \pmod 6$ donc $7x\equiv 3 \pmod 6$.

b) $7\equiv 1 \pmod 6$ donc $x\equiv 3 \pmod 6$.

c) $7x\equiv 3 \pmod 6$ et $x_0\equiv 3 \pmod 6$ d'où :

$$7(x-3)\equiv 0 \pmod 6.$$

d) 6 divise $7(x-3)$ et 6 est premier avec 7 ; donc 6 divise $x-3$ et $x=6k+3$ $(k\in\mathbb{Z})$.

2. Si $x=6k+3$, $7(6x+3)+6y=3$; soit $6y=-42x-18$; d'où $y=-7x-3$ $(k\in\mathbb{Z})$.

97 **1.** On a $57x=10y=0$.

D'après le théorème de Gauss, 57 divise y.

Donc $y=57k$ et $x=10k$ $(k\in\mathbb{Z})$.

2. Par hypothèse, $57x_0-10y_0=m$.

Donc $57(x-x_0)=10(y-y_0)$ (2).

Dans ce cas, $y=57k+y_0$ et $x=10k+x_0$.

3. a) $57x-10y=1$ (3)

Comme 57 et 10 sont premiers entre eux, l'équation (3) a des solutions.

b) On pose $a=57$ et $b=10$.

$57=5\times 10+7$; $7=a-5b$;

$10=1\times 7+3$; $3=6b-a$.

$7=2\times 3+1$ soit $3-5b=2(6b-a)+1$.

D'où $3a-17b=1$. Donc $x_0=3$ et $y_0=17$ est solution de (3).

c) Ainsi $x=10k+3$ et $y=57k+17$.

98 *Corrigé sur le site élève.*

99 **1. a)** $a^2-2b^2=1$ équivaut à $a(a)-b(2b)=1$; donc, d'après le théorème de Bézout, PGCD$(a\,;\,b)=1$.

b) $a^2=2b^2+1$; donc a est impair car a^2 est impair.

c) $a=2p+1$, $4p^2+4p+1-1=2b^2$ et $b^2=2p(p+1)$.

b^2 est pair donc b est pair.

2. $A^2-2B^2=9a^2+24ab+16b^2-8a^2-24ab-18b^2$

$=(a^2-2b^2)=1$.

Donc $(A\,;\,B)$ est un couple solution.

3. $(577\,;\,408)$ est un couple solution.

100 **1.** $x^2-3y-4=0$ implique $x^2\equiv 1 \pmod 3$; soit $x=3k+1$ ou $x=3k+2$;

si $x=3k+1$; $y=3k^2+2k-1$;

si $x=2k+2$, $y=3k^2+4k$.

On vérifie que ces solutions conviennent.

2. Si $x^2-3y-5=0$, alors $x^2\equiv 2 \pmod 3$ ce qui est impossible.

CHIFFREMENT AFFINE

101 **1.** INFINI se code XYMXYX.

2. a) $21\times 5\times x\equiv 5z \pmod{26} \Leftrightarrow 105x\equiv 5z \pmod{26}$; soit $x\equiv 5z \pmod{26}$.

b) $x\equiv 5(y-11) \pmod{26}$; $x\equiv 5y+23 \pmod{26}$; d'où $y\mapsto x=5y+23$.

c) LDXUXR se décode AMITIÉ.

102 **1.** E correspond à 4 ; donc $4=4a+b \pmod{26}$.

J associé à 9 est codé N associé à 13 ; donc :

$$13=9a+b \pmod{26}.$$

2. a) $\left.\begin{array}{l}9a+b\equiv 13 \pmod{26}\\ 4a+b\equiv 4 \pmod{26}\end{array}\right\}\Rightarrow 5a\equiv 9 \pmod{26}$

$5\times 5a=45 \pmod{26}$, soit $-a\equiv 19 \pmod{26}$ donc $a\equiv 7 \pmod{26}$.

b) $b \equiv 4 - 4a \pmod{26}$, soit $b \equiv -24 \pmod{26}$ donc $b \equiv 2 \pmod{26}$.
D'où $f(x) = 7x + 2$.

3. a) $7(15y + 22) + 2 = 105y + 156$; soit :
$$105y + 156 \equiv y \pmod{26}.$$
Donc, la fonction de décodage est $y \mapsto x = 15y + 22$.

b) Le message décodé est :

BONJOUR À TOUS.

AVEC LE PPCM

103 *Corrigé sur le site élève.*

104 **1.** $x^2 + y^2 = 4\,625$ $(x < y)$.
On pose $x = \Delta x'$ et $y = \Delta y'$ avec PGCD $(x' ; y') = 1$.
Donc $\Delta^2(x'^2 + y'^2) = 4\,625$ et $440 = \Delta x'y'$.
Δ^2 divise $4\,625 = 37 \times 5^3$, donc Δ^2 divise 5^2, soit $\Delta = 1$ ou 5.
2. • Si $\Delta = 1$, $x'^2 + y'^2 = 4\,625$ et $x'y' = 440$.
Soit $x'^2 + y'^2 + 2x'y' = (x' + y')^2 = 5\,505$.
5 505 n'est pas un carré d'un entier.
• Si $\Delta = 5$, $x'^2 + y'^2 = 185$ et $x'y' = 88$ soit $(x' + y')^2 = 361$ et $x' + y' = 19$.
$(x' - y')^2 = 185 - 176 = 9$
soit $y' - x' = 3$
$y' + x' = 19$
donc $y' = 11$ et $x' = 8$.
Donc, le seul point M a pour coordonnées (40 ; 55).

AVEC LES TICE

105 $y_1 = 9x_1 + 4x_2 \pmod{26}$
$y_2 = 5x_1 + 7x_2 \pmod{26}$

1. a) et **b)** IMAGES se code QVYQEQ et des lettres différentes donnent des codes identiques.
On constate la même chose avec les autres codages.

2. a) $\begin{cases} y_1 = 9x_1 + 4x_2 \ (\times 7) \text{ puis } (\times -5) \\ y_2 = 5x_1 + 7x_2 \ (\times -4) \text{ puis } (\times 9) \end{cases}$

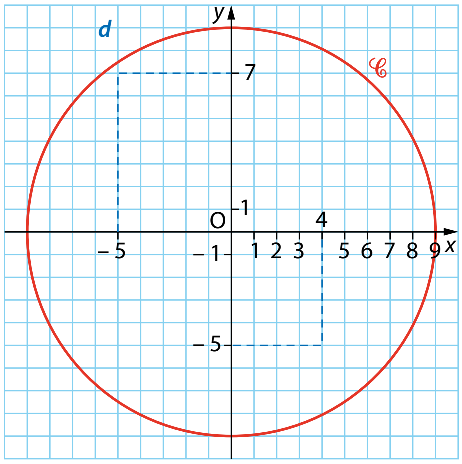
alors $\begin{cases} 7y_1 - 4y_2 \equiv 43x_1 \pmod{26} \\ -5y_1 + 9y_2 \equiv 43x_2 \pmod{26} \end{cases}$

b) $43p + 26q = 1$ et PGCD $(43 ; 26) = 1$; donc p et q existent.
c) $a = 43$ et $b = 26$;
$43 = 1 \times 26 + 17$, donc $17 = a - b$;
$26 = 1 \times 17 + 9$, soit $9 = 2b - a$;
$17 = 1 \times 9 + 8$, soit $8 = 2a - 3b$;
$9 = 8 + 1$, soit $1 = 5b - 3a$;
$p = -3$ ou $p = 23$.
d) Soit $43 \times 23x_1 = 23 \times 7y_1 - 4 \times 23y_2$;
D'où $x_1 \equiv 5y_1 - 14y_2 \equiv 5y_1 + 12y_2 \pmod{26}$.
De même $x_2 \equiv 15y_1 + 25y_2 \pmod{26}$.
e) On décode BHZHVKK en :

LIBERTÉ

Prendre toutes les initiatives

106

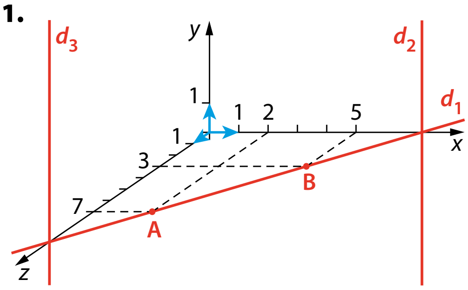


On trace la droite d d'équation $4x + 3y = 1$ et le cercle $\mathscr{C}$ de centre O et de rayon 9.
Résolvons l'équation $4x + 3y = 1$.
Soit $4(1 - x) = 3(1 + y)$ d'où $y = 4k - 1$ et $x = 1 - 3k$ $(k \in \mathbb{Z})$.
De plus, $(1 - 3k)^2 + (x + 4k)^2 \leqslant 81$.
C'est-à-dire : $25k^2 - 14k - 79 \leqslant 0$.
D'où $k \in \{-1 ; 0 ; 1 ; 2\}$.
Donc, les points de d ont pour coordonnées :
$$(4 ; 5) ; (1 ; -1) ; (-2 ; 3) ; (-5 ; 7).$$

107 $\begin{cases} A = 4a + 7b \\ B = 5a + 9b \end{cases} \Leftrightarrow \begin{cases} a = 9A - 7B \\ b = 4B - 5A \end{cases}$

Tout diviseur de a et b divise toute combinaison linéaire, donc A et B. De même, tout diviseur de A et B divise a et b. D'où :
$$\text{PGCD}(a ; b) = \text{PGCD}(A ; B) = 7$$

108 **1.**



2. d_1 est la droite d'intersection d'équation :
$$3x + 4y = 29.$$
Le couple (7 ; 2) est solution de l'équation ; donc :
$$3(x - 7) = 4(2 - y).$$
Donc $x = 4k + 7$ et $y = 2 - 3k$.
• $y \geqslant 0$, $2 - 3k \geqslant 0$ $\left(k \leqslant \dfrac{2}{3}\right)$
• $x \geqslant 0$, $4k + 7 \geqslant 0$ $\left(k \geqslant -\dfrac{7}{4}\right)$
D'où $k \in \{-1 ; 0\}$.
Les points dont les coordonnées sont à la fois entières et positives sont :
$$A(7 ; 2) \text{ et } B(3 ; 5).$$

EXERCICES Le jour du BAC (page 70)

109 *Corrigé sur le site élève.*

110 **A.** • Si a est premier avec b alors il existe des entiers relatifs u et v tels que : $au + bv = 1$.
Donc $(ac)u + (bc)v = c$.
a divise bc et ac donc a divise c.
• $a = pk$ et $a = qk'$, donc $pk = qk'$.
p divise qk' et $\text{PGCD}(p\ ;\ q) = 1$; donc p divise k', soit $k' = \lambda p$ et $a = pq\lambda$.
Donc pq divise a et $a \equiv 0 \pmod{pq}$.

B. 1. a) $17u + 5v = 1$ (1) ;
17 et 5 sont premiers entre eux ; il existe donc au moins un couple $(u\ ;\ v)$ vérifiant (1).
b) $17u \times 3 = 3 - 3 \times 5v$ et $9 \times 5v = 9 - 9 \times 17u$.
Donc $n_0 = 3 + 6 \times 5v = 9 - 6 \times 17u$.
Soit $n_0 \equiv 3 \pmod 5$ et $u_0 \equiv 9 \pmod{17}$; d'où $n_0 \in \mathcal{S}$.
c) $17 \times -2 + 5 \times 7 = 1$, donc $(u\ ;\ v) = (-2\ ;\ 7)$ vérifie (1) ; d'où $n_0 = 17 \times -6 + 9 \times 35 = 315 - 102 = 213$.
n_0 est solution de $\mathcal{S}$.

2. a) $n - n_0 \equiv 0 \pmod{17}$ et $n - n_0 \equiv 0 \pmod 5$.
Or 17 et 5 sont premiers entre eux ; donc $n - n_0 \equiv 0 \pmod{85}$.
b) $n = 213 + 85k$; or $213 \equiv 43 \pmod{85}$ donc $n = 43 + 85k$ $(k \in \mathbb{Z})$.
Réciproquement, si $n = 43 + 85k$ alors :
$$n \equiv 9 \pmod{17} \text{ et } n \equiv 3 \pmod 5.$$

3. Si n est le nombre de jetons, on a :
$$300 \leqslant n \leqslant 400\ ;\ n \equiv 9 \pmod{17} \text{ et } n \equiv 3 \pmod 5.$$
$300 \leqslant 43 + 85k \leqslant 400$.
$257 \leqslant 85k \leqslant 357$.
Seul $k = 4$ convient. Donc, Zoé a donc $43 + 340 = 383$ jetons.

111 **1.** $a_{n+1} = a_n + 2$ donc (a_n) est une suite arithmétique de premier terme.
$a_1 = 3$, de raison 2 ; donc :
$$a_n = 3 + (n-1)2 = 2n + 1.$$
2. a) Démontrons que, pour tout $n \in \mathbb{N}^*$:
$$b_n = 2 + \sum_{i=1}^{n-1} a_i.$$
Pour $n = 1$, $b_1 = 2$ donc vrai.
Si $b_n = 2 + \sum_{i=1}^{n-1} a_i$, alors :
$$b_{n+1} = b_n + a_n = 2 + \sum_{i=1}^{n-1} a_i + a_n.$$
Soit $b_{n+1} = 2 + \sum_{i=1}^{n} a_i$.
Donc, pour tout $n \geqslant 1$, la proposition est vraie.
b) Il en résulte que :
$$b_n = 2 + \frac{n-1}{2}[3 + 2n - 1] = 2 + n^2 - 1,$$
d'où $b_n = n^2 + 1$.
3. a) Si d divise $n^2 + 1$ et $2n + 1$, d divise :
$$2(n^2 + 1) - n(2n + 1) = 2 - n\ ;$$
donc d divise $2 - n$ et $2n + 1$; soit d divise :
$$(2n + 1) + 2(2 - n) = 5.$$
Donc d divise 5.
b) $a_n \equiv 0 \pmod 5$, si et seulement si, $2n \equiv 4 \pmod 5$.

$n \equiv$	0	1	2	3	4
$2n \equiv$	0	2	4	1	3

Donc $n \equiv 2 \pmod 5$.
De même, si $n \equiv 2 \pmod 5$, $n^2 \equiv 4 \pmod 5$ et $b \equiv 0 \pmod 5$.
Donc $\text{PGCD}(a_n\ ;\ b_n) = 5$.
c) Dans les autres cas, $\text{PGCD}(a_n\ ;\ b_n) = 1$.

112 **1. a)** Si $u = 2$ et $v = 3$, on a : $11 \times 2 - 7 \times 3 = 1$.
Donc, le couple $(2\ ;\ 3)$ est solution de l'équation :
$$11x - 7y = 1.$$
b) Du **a)** on déduit que :
$$11 \times 10 - 7 \times 15 = 5.$$
Donc $(10\ ;\ 15)$ est une solution particulière de **(E)**.
Donc $11(x - 10) = 7(y - 15)$.
7 divise $(x - 10)$ car 7 divise $11(x - 10)$ et 7 est premier avec 11 ; soit :
$$x = 7k + 10 \text{ et } y = 11k + 15\ (k \in \mathbb{Z}).$$
c) x et y appartiennent à l'intervalle $[0\ ;\ 50]$ si, et seulement si, $k \in \{-1\ ;\ 0\ ;\ 1\ ;\ 2\ ;\ 3\}$.
Les points de d qui conviennent ont donc pour coordonnées :
$(3\ ;\ 4)$; $(10\ ;\ 15)$; $(17\ ;\ 26)$; $(24\ ;\ 37)$ et $(31\ ;\ 48)$.

2. a) $11x^2 \equiv x^2 \pmod 5$; soit $7y^2 \equiv 2y^2 \pmod 5$;
donc $x^2 - 2y^2 \equiv 0 \pmod 5$.
b) Tableau des restes modulos :

$n \equiv$	0	1	2	3	4
$n^2 \equiv$	0	1	4	4	1
$2n^2 \equiv$	0	2	3	3	2

Ainsi, les restes :
– de la division de x^2 par 5 peuvent être : 0 ; 1 ; 4 ;
– de la division de $2y^2$ par 5 peuvent être : 0 ; 2 ; 3.
c) Si $(x\ ;\ y)$ est solution de **(F)** alors x et y sont congrus 0 modulo 5. Ils sont donc des multiples de 5.

3. Si $x \equiv 0 \pmod 5$ et $y \equiv 0 \pmod 5$, $x = 5k$ et $y = 5k'$, donc :
$$25 \times 11k^2 - 25 \times 7k'^2 = 5$$
$$5[11k^2 - 7k'^2] = 1$$
Ce qui n'est pas possible car 5 ne divise pas 1.
Il en résulte que l'équation (E) n'a pas de solutions.

113 **1.** $u_1 = 5 \times 14 - 6 = 64$.
$u_2 = 5 \times 64 - 6 = 320 - 6 = 314$.
$u_3 = 5 \times 314 - 6 = 1\,570 - 6 = 1\,564$.
$u_4 = 5 \times 1\,564 - 6 = 7\,820 - 6 = 7\,814$.
Il semble que, si n est pair, les deux derniers chiffres de u_n sont 14 et si n est impair, les deux derniers chiffres de u_n sont 64.

2. a) $u_{n+2} = 5u_{n+1} - 6 = 5(5u_n - 6) - 6$

$u_{n+2} = 25u_n - 36.$

Donc $u_{n+2} \equiv u_n \pmod 4$ (1)

b) D'après (1), $u_{2k} \equiv u_2 \pmod 4$.

Donc $u_{2k} \equiv 2 \pmod 4$ et $u_{2k+1} \equiv u_1 \pmod 4$

soit $u_{2k+1} \equiv 0 \pmod 4$.

3. a) Pour $n = 0$, $2u_0 = 25 + 3 = 28$.

Comme $u_0 = 14$, la proposition est vraie pour $n = 0$.

Si $2u_n = 5^{2n+2} + 3$, alors :

$2u_{n+1} = 2(5u_n - 6) = 10u_n - 12 = 5(5^{n+2} + 3) - 12$

$2u_{n+1} = 5^{n+3} + 3.$

La proposition est vraie pour $n + 1$. Elle est donc vraie pour tout n de $\mathbb{N}$.

b) Pour $n = 0$, $2u_0 = 25 + 3 = 28$.

Si $n \geqslant 1$, $5^{n+2} \equiv 25 \pmod{100}$;

donc, pour tout n de $\mathbb{N}$, $2u_n \equiv 28 \pmod{100}$;

4. Donc $2u_n = 100k + 28$ et $u_n = 50k + 14$.

• Si $k = 2p$, $u_n \equiv 100p + 14$, donc $u_n \equiv 14 \pmod{100}$; les deux derniers chiffres sont 1 et 4 ;

• Si $k = 2p + 1$, $u_n \equiv 100p + 64$, donc $u_n \equiv 64 \pmod{100}$; les deux derniers chiffres sont 6 et 4.

5. Tout diviseur de deux entiers consécutifs divise la différence, donc divise 50.

Or, aucun diviseur de 50 ne divise deux entiers consécutifs.

Donc ils sont premiers entre eux.

EXERCICES Pour aller plus loin (page 72)

114 **1.** Si $n = 3$, $x^2 \equiv 4 \pmod 5$; donc, la proposition est fausse.

Si $x^2 \equiv 1 \pmod 5$, on peut avoir $x = 6$ ou $x = 9$; donc x n'est pas nécessairement impair.

2. Si $8a - 13b = 6$, alors $\text{PGCD}(a\,;\,b) = 6$.

La proposition est fausse : en prenant $a = 4$ et $b = 2$, on a $8a - 13b = 16$ et $\text{PGCD}(a\,;\,b) = 2$.

Réciproquement, si $\text{PGCD}(a\,;\,b) = 6$, alors $8a - 13b = 6$.

La proposition est vraie. On peut trouver a' et b' tels que : $8a' - 13b' = 1$.

3. Si $a = 7$ et $b = 4$ alors $a \equiv b \pmod 3$; mais comme a^2 n'est pas congru b^2 modulo 9, la proposition est fausse, ainsi que la réciproque ($a^2 = 49$; $b^2 = 4$).

4. Si $a = 2$ et $b = 3$, 6 divise ab ; mais comme 6 ne divise pas a ou b, la proposition est fausse.

5. Si a est premier avec bc, alors il est premier avec b.

La proposition est vraie car $au + bcv = 1$; donc $au + b(cv) = 1$.

Ainsi, a est premier avec b.

La réciproque est fausse ; car, par exemple, $a = 3$, $b = 5$ et $c = 6$.

$$\text{PGCD}(a\,;\,b) = 1 \text{ et } \text{PGCD}(a\,;\,bc) = 3.$$

6. La proposition est fausse $\frac{2}{3}$ et $\frac{3}{5}$ sont irréductibles mais $\frac{6}{15}$ ne l'est pas.

La réciproque est vraie.

115 $31j + 12m = 723$ soit $31j = 3[241 - 4m]$.

3 divise $31j$ et 3 est premier avec 31 ; donc 3 divise j ; on a :

$$j = 3k \text{ et } 4m = 241 - 31k.$$

$241 - 31k \equiv 0 \pmod 4$ soit $3k = 1 \pmod 4$.

Il en résulte que $k \equiv 3 \pmod 4$.

$k = 4p + 3$; de plus $1 \leqslant k \leqslant 7$, donc $k = 3$ ou $k = 7$.

• Si $k = 3$: $4m = 241 - 93 = 148$.

Donc $m = 37 > 12$, ne convient pas.

• Si $k = 7$, $j = 21$ et $4m = 241 - 217 = 24$. Donc $m = 6$.

Il s'agit donc du 21 juin.

116 **1.** Tout diviseur d commun à x et y divise toute combinaison linéaire du type $\alpha x + \beta y$; donc d divise A et B.

2. a) $x = 3\text{A} - \text{B}$ et $y = \text{B} - 2\text{A}$.

b) Tout diviseur de A et B divise toute combinaison linéaire de ces nombres ; donc x et y.

3. Si δ est le PGCD de x et y et Δ celui de A et B, alors :

$$\delta \leqslant \Delta \text{ et } \Delta \leqslant \delta \,;\, \text{donc } \delta = \Delta.$$

4. $a = 2^n + 3^n$ et $b = 2 \times 2^n + 3 \times 2^n$.

Si on pose $x = 2^n$ et $y = 3^n$, on a :

$$a = x + y \text{ et } b = 2x + 3y.$$

Il en résulte que $\text{PGCD}(a\,;\,b) = \text{PGCD}(2^n\,;\,3^n) = 1$.

117 **1.** $n\binom{n-1}{p-1} = n\dfrac{(n-1)!}{(p-1)!(n-1)!} = \dfrac{n!}{(p-1)!(n-p)!}$

$$n\binom{n-1}{p-1} = \frac{n!\,p}{p!(n-p)!} = p\binom{n}{p}$$

Donc $p\binom{n}{p} = n\binom{n-1}{p-1}$.

2. n et p sont premiers entre eux et n divise $p\binom{n}{p}$ donc n divise $\binom{n}{p}$.

118 **1.** $\dfrac{3a^3}{b^3} + \dfrac{4a^2}{b^2} + \dfrac{2a}{b} - 4 = 0$, soit :

$$3a^3 + 4a^2b + 2ab^2 - 4b^3 = 0$$

$$a(3a^2 + 4ab + 2b^2) = 4b^3.$$

a étant premier avec b^3, alors a divise 4 ;

et $b(4b^2 - 2ab - 4a^2) = 3a^3$.

b étant premier avec a, b divise 3.

2. $a \in \{-2\,;\,-1\,;\,1\,;\,2\,;\,-4\,;\,4\}$ et $b \in \{-3\,;\,3\}$.

Donc $\dfrac{a}{b}$ peut prendre les valeurs :

$$-\frac{2}{3}\,;\,\frac{1}{3}\,;\,-\frac{1}{3}\,;\,-\frac{2}{3}\,;\,\frac{4}{3}\,;\,-\frac{4}{3}.$$

On vérifie que $x = \frac{2}{3}$ est solution ; on a :

$$\frac{8}{9} + \frac{16}{9} + \frac{4}{3} - 4 = 4 - 4 = 0.$$

$3x^3 + 4x^2 + 2x - 4 = (3x - 2)(x^2 + 2x + 2)$ et $x^2 + 2x + 2 = 0$ n'a pas de solution réelle.

Donc $x = \frac{2}{3}$ est l'unique solution.

On peut également établir le tableau de variation de f, définie sur $\mathbb{R}$, par :

$$f(x) = 3x^3 + 4x^2 + 2x - 4$$

x	$-\infty$	$\frac{2}{3}$	$+\infty$
f'		+	
f	$-\infty$	0	$-\infty$

Ainsi, le théorème des valeurs intermédiaires $\frac{2}{3}$ est la seule solution.

ÉQUATIONS DIOPHANTIENNES

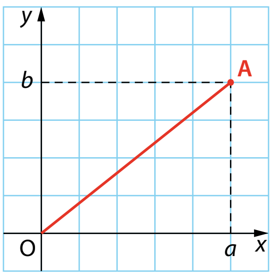
119 **1.** $\left.\begin{matrix} 7x - 4y = 1 \\ 7 \times 3 - 4 \times 5 = 1 \end{matrix}\right\}$ soit $7(x - 3) = 4(y - 5)$. Donc :

$$x = 4k + 3 \text{ et } y = 7k + 5.$$

avec $0 \leqslant x \leqslant 4$ et $0 \leqslant y \leqslant 5$.

Ainsi, le point de coordonnées (3 ; 5) est le seul point du réseau $\mathcal{R}(4 ; 7)$.

2. a)



$M(x ; y) \in [OA]$ si, et seulement si :

$$0 \leqslant x \leqslant a ; \; 0 \leqslant y \leqslant b$$

et $bx - ay = 0$ qui est l'équation de la droite (OA).

b) $bx = ay$.

• PGCD $(a ; b) = 1$, a divise bx ; donc a divise x :

$$x = ak \text{ et } b = bk.$$

Donc O(0 ; 0) et A(a ; b) sont les seuls points du réseaux appartenant à [OA].

• PGCD$(a ; b) = \Delta$, donc $a = \Delta a'$ et $b = \Delta b'$.

PGCD$(a' ; b') = 1$, donc $b'x = a'y$, soit $x = qa'$ et $b = qb'$.

Il existe donc q points appartenant au réseau.

c) PGCD (364 ; 308) = PGCD (13×28 ; 11×28) = 28.

Donc $0 \leqslant x \leqslant 308$ et $0 \leqslant y \leqslant 364$.

On a $11y = 13k$, soit $x = 11k$ et $y = 13k$.

Il existe donc 28 points appartenant au réseau.

120 **1.** Soit (E) : $6x + 7y = 57$.

$6(-57) + 7(57) = 57$ soit $6(x + 57) = 7(57 - y)$.

D'où $x = 7k - 57$ et $y = 57 - 6k$ $(k \in \mathbb{Z})$.

2. $\mathcal{P}$: $6x + 7y + 8z = 57$.

Un point appartient à $(O ; \vec{i} ; \vec{j})$ si $z = 0$; d'où :

$$x = 7k - 57 \text{ et } y = 57 - 6k.$$

$x \geqslant 0$ et $y \geqslant 0$ soit $k \geqslant 9$ et $k \leqslant 9$.

Donc $k = 9$ et le point a pour coordonnées (6 ; 3).

3. a) $2(3x + 4z) + 7y = 57$.

57 est impair et $2(3x + 4z)$ est pair ; donc y est impair.

b) $y = 2p + 1$, donc $6x + 14p + 7 + 8z = 57$.

$6x + 8z + 14p - 50 = 0$

$3x + 4z + 7p - 25 = 0$

donc $z + p \equiv 1 \pmod 3$.

c) On pose $p + z = 3q + 1$

$$3x + 4(3q + 1 - p) + 7p - 25 = 0$$
$$3x + 12q + 4 + 3p - 25 = 0$$
$$3x + 3p + 12q - 21 = 0$$

D'où $x + p + 4q = 7$.

$p \geqslant 0$, $x \geqslant 0$, $q \geqslant 0$, donc $4q \leqslant 7$; soit $q = 0$; ou $q = 1$.

d) • Si $q = 0$: $x = 7 - p$, $z = 1 - p$ et $y = 1 + 2p$.

Soient les points de coordonnées :

$$(7 ; 1 ; 1) \;\; (6 ; 3 ; 0).$$

• Si $q = 1$: $x = 3 - p$, $y = 1 + 2p$ et $z = 4 - p$.

Les points de $\mathcal{P}$, dont les coordonnées sont des entiers naturels, sont :

$$(3 ; 1 ; 4) ; (2 ; 3 ; 3) ; (1 ; 5 ; 2) ; (0 ; 7 ; 1).$$

121 **1. a)** $(S) \begin{cases} N \equiv 5 \pmod{13} \\ N \equiv 1 \pmod{17} \end{cases} \Leftrightarrow (S_1) \begin{cases} N = 17x + 1 \\ N = 13y + 5 \end{cases}$

$$(S_1) \Leftrightarrow (S_2) \begin{cases} N = 17x + 1 \\ 17x - 13y = 4 \end{cases}$$

b) $17x - 13y = 4$ et $17(-12) - 13(-16) = 4$; donc :

$$17(x + 12) = 13(y + 16)$$

Il en résulte que :

$$x = 13k - 12 \text{ et } y = 17k - 16, \; k \in \mathbb{N}.$$

2. a) Soit $N = 221k - 203$.

Or $-203 \equiv 18 \pmod{221}$, d'où $N = 221k + 18$.

b) $N \equiv 18 \pmod{221} \Leftrightarrow N = 221k + 18$; donc :

$$N \equiv 5 \pmod{13} \text{ et } N \equiv 1 \pmod{17}.$$

122 **1.** On note x et y respectivement le nombre d'étudiants et le nombre d'enfants. Il y a donc $28 - (x + y)$ adultes ; soit :

$$26(28 - x - y) + 17x + 13y = 613.$$

En développant, on obtient :

$$(E) \quad 9x + 13y = 115.$$

2. a) $9x + 13y = 1$ a pour solution particulière :

$$x = 3 \text{ et } y = -2.$$

b) Donc $x = 345$ et $y = -230$ est une solution particulière de (E).

Donc $9(x - 345) + 13(y + 230) = 0$,

soit $9(345 - x) = 13(y + 230)$.

Il en résulte que :

$$x = 345 - 13k \text{ et } y = 9k - 230.$$

c) $x \geqslant 0$ et $y \geqslant 0$, donc seul $k = 26$ convient.

Il y a donc 7 étudiants, 4 enfants et 17 adultes.

123 On suppose que x fléchettes sont dans le 12 et y dans le 5. On a donc :

$$12x + 5y = 200$$

équivalent à $12x = 5(40 - y)$.

5 divise $12x$ et 5 premier avec 12, donc 5 divise x :

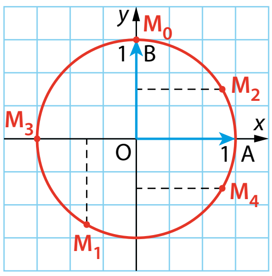
$$x = 5k \text{ et } y = 40 - 12k \ (k \in \mathbb{N}).$$

$y \geqslant 0$ donc $k \in \{0\ ;1\ ;2\ ;3\}$.

Ainsi les couples $(x\ ;y)$ possibles sont :

$$(0\ ;40)\ ;(5\ ;28)\ ;(10\ ;16)\ ;(15\ ;4).$$

124 **1.**



2. $z_0 = e^{i\left(\frac{\pi}{2}+0\right)} = e^{i\frac{\pi}{2}} = i$;

si $z_n = e^{i\left(\frac{\pi}{2}+\frac{5n\pi}{6}\right)}$ alors $z_{n+1} = z_n e^{i\frac{5\pi}{6}} = e^{i\left(\frac{\pi}{2}+\frac{5n\pi}{6}\right)} e^{i\frac{5\pi}{6}}$

soit $z_{n+1} = e^{i\left(\frac{\pi}{2}+\frac{5(n+1)\pi}{6}\right)}$.

Donc, pour tout n de $\mathbb{N}$:

$$z_n = e^{i\left(\frac{\pi}{2}+\frac{5n\pi}{6}\right)}.$$

3. $M_n = M_p \Leftrightarrow e^{i\left(\frac{\pi}{2}+\frac{5n\pi}{6}\right)} = e^{i\left(\frac{\pi}{2}+\frac{5p\pi}{6}\right)} = e^{2k\pi}$

soit $\dfrac{5n\pi}{6} = \dfrac{5p\pi}{6} = 2k\pi$

d'où $5(n - p) = 12k$ et $5(n - p) \equiv 0 \pmod{12}$

d'où $n - p \equiv 0 \pmod{12}$,

car 12 premier avec 5 divise $(n - p)$.

4. a) $12x - 5y = 3$, $12 \times 4 - 5 \times 9 = 3$,

d'où $12(x - 4) = 5(y - 9)$

donc $x = 5k + 4$ et $y = 12k + 9$.

b) M_n appartient à la demi-droite $[Ox)$ si, et seulement si :

$$\frac{\pi}{2} + \frac{5n\pi}{6} = 2k\pi$$

soit $3 + 5n = 12k$ où $12k - 5n = 3$.

D'après **4. a)** : $n = 12k + 9$ $(k \in \mathbb{N})$.

125 **1.** AMICAL se code KYUIHW.

2. a) $\begin{cases} y_1 = 5x_1 + 3x_2 \ (\times 7) \\ y_2 = 7x_1 + 2x_2 \ (\times -5) \end{cases}$ ou $\begin{matrix} (\times -2) \\ (\times\ 3) \end{matrix}$

Il vient :

$$11x_2 = 7y_1 - 5y_2 \text{ et } 11x_1 = 3y_2 - 2y_1.$$

b) $11u + 26v = 1$, soit $11(-7) + 26(3) = 1$.

D'où $11(u + 7) = 26(3 - v)$.

Il en résulte que :

$$u = 26k - 7 \text{ et } v = 3 - 11k.$$

c) Donc $u \equiv -7 \pmod{26}$.

Or $11x_1 = -2y_1 + 3y_2$, donc :

$$11(-7)x_1 = 14y_1 - 21y_2.$$

Donc, la congruence modulo 26 est :

$$x_1 = 14y_1 + 5y_2.$$

d) $11(-7)x_2 = -49y_1 + 35y_2$, d'où :

$$x_2 = 3y_1 + 9y_2.$$

3. DCAMSZXG se décode en :

À BIENTÔT.