

Chapitre 13

Arithmétique

dans $\mathbb{Z}$

Du niveau de base au niveau concours

À connaître par cœur

$$a \equiv b [n] \iff n \mid a - b$$
$$a = bq + r \text{ avec } 0 \leq r < |b|$$

Défi de concours $F_n = 2^{2^n} + 1$: deux à deux premiers entre eux ? Et $641 \mid F_5$?

$$14 \equiv 2 [12]$$



$$-10 \equiv 2 [12]$$

L'arithmétique des horloges : la congruence modulo n

★★★★ Niveau 4 · Concours

★★★ Niveau 3 · Approfondissement

★★ Niveau 2 · Bac

★ Niveau 1 · Bases

Cours complet

Méthodes et pièges

66 exercices corrigés

Test d'entrée

Sommaire

Test d'entrée : par où commencer ?	4	19 Niveau 4 · Concours	27
1 Divisibilité dans $\mathbb{Z}$	5	20 Divisibilité et division euclidienne	29
2 La division euclidienne	6	21 Congruences	30
3 Raisonner sur les restes	7	22 Nombres premiers	32
4 Congruence modulo n	8	23 PGCD et PPCM	34
5 Calculer avec les congruences	10	24 Équations en nombres entiers	36
6 Les nombres premiers	11	25 Défis de concours	37
7 Décomposition en facteurs premiers	13	26 Corrigés du niveau 1	40
8 Le PGCD	14	27 Corrigés du niveau 2	43
9 Le PPCM	16	28 Corrigés du niveau 3	45
10 Nombres premiers entre eux	17	29 Corrigés du niveau 4	47
11 Équations dans $\mathbb{Z}$	18	30 Corrigés : divisibilité et restes	50
12 Pour aller plus loin	19	31 Corrigés : congruences	53
13 Les pièges classiques	19	32 Corrigés : nombres premiers	56
14 Les astuces des concours	20	33 Corrigés : PGCD et PPCM	59
15 L'essentiel du chapitre en une page	22	34 Corrigés : équations en entiers	62
16 Niveau 1 · Bases	23	35 Corrigés : défis de concours	65
17 Niveau 2 · Bac	24	26 Corrigé du test d'entrée	68
18 Niveau 3 · Approfondissement	26		

Comment utiliser ce livret

Les 4 niveaux d'exercices

Niveau 1 · Bases ★

les automatismes indispensables.

Niveau 2 · Bac ★★

le niveau des devoirs surveillés.

Niveau 3 · Approfondissement ★★★

pour viser la mention Très bien.

Niveau 4 · Concours ★★★★★

problèmes de concours (classes préparatoires, écoles d'ingénieurs).

Les encadrés du cours

Définition : à savoir par cœur.

Propriété / Théorème : les outils.

Méthode : la démarche pas à pas.

Exemple : un calcul entièrement rédigé.

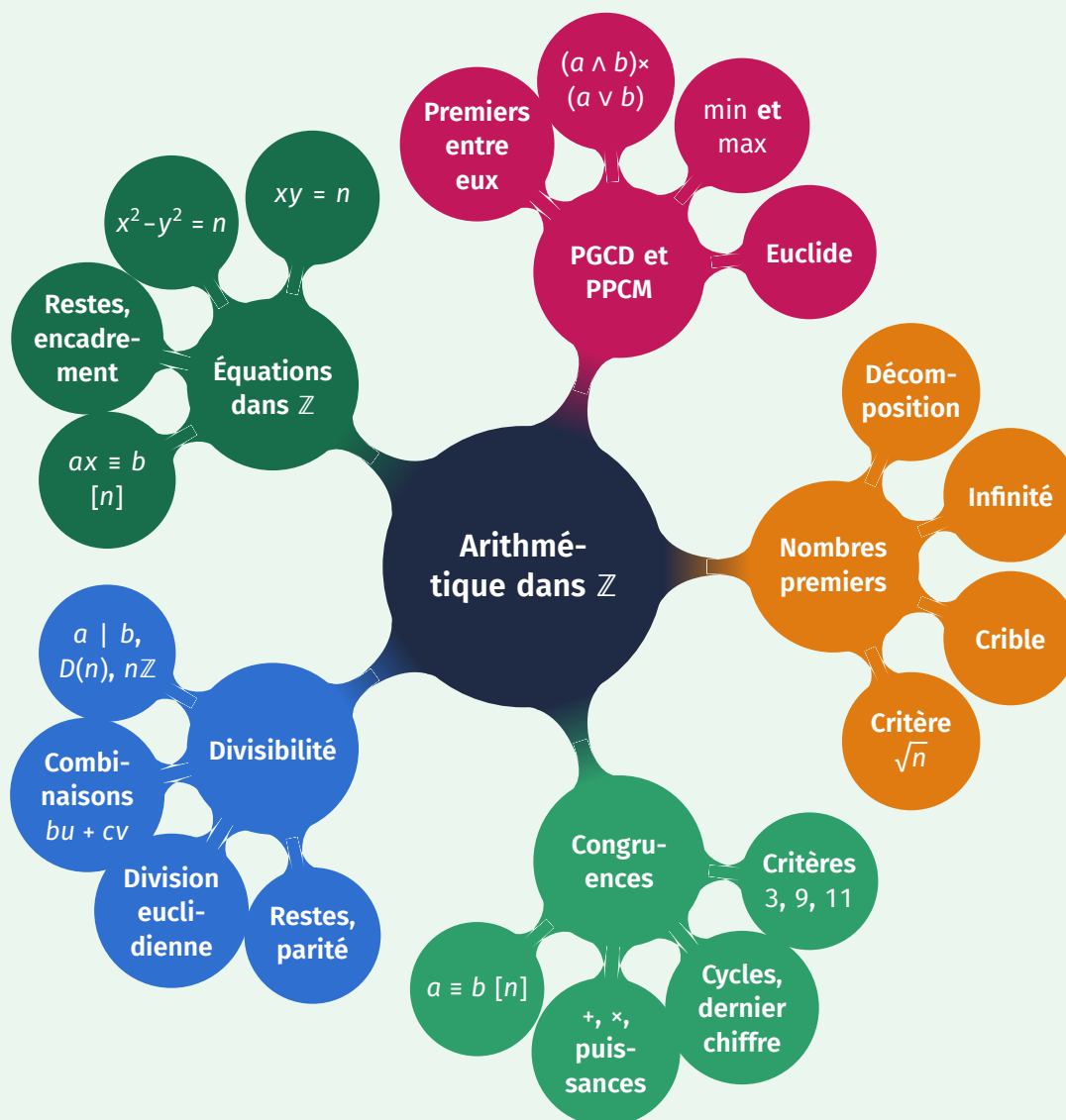
Piège : l'erreur classique à éviter.

Astuce de concours ★ : le petit plus qui fait gagner du temps.

Ce livret est « intelligent » : commence par le **test d'entrée** (page 4) ; en 15 minutes, il t'indique par où commencer et quels exercices faire en priorité. Le livret contient 66 exercices corrigés : la partie B est un parcours en 4 niveaux (exercices 1 à 30) ; la partie C est une banque de 36 exercices classés par thème (Divisibilité et division euclidienne, Congruences, Nombres premiers, PGCD et PPCM, Équations en nombres entiers, Défis de concours). Tous les corrigés sont regroupés dans la partie D.

Conseil : cherche chaque exercice au moins 10 minutes avant de lire le corrigé. Le numéro de page du corrigé est indiqué à droite de chaque énoncé (il est cliquable dans le PDF).

La carte du chapitre



À la fin du chapitre, je sais...

- | | |
|---|---|
| ☐ utiliser $a \mid b$ et les combinaisons $bu + cv$; | ☐ reconnaître un nombre premier (critère $\sqrt{n}$) ; |
| ☐ trouver les n tels que $A(n) \mid B(n)$; | ☐ décomposer, compter les diviseurs ; |
| ☐ effectuer une division euclidienne dans $\mathbb{Z}$; | ☐ calculer un PGCD (Euclide, décomposition) ; |
| ☐ raisonner sur les restes (carrés modulo 3, 4, 8) ; | ☐ calculer un PPCM, utiliser $(a \wedge b)(a \vee b) = ab $; |
| ☐ calculer avec les congruences ; | ☐ utiliser $a \wedge b = 1$ et $a = da'$, $b = db'$; |
| ☐ trouver le reste d'une grande puissance ; | ☐ résoudre $xy = n$, $x^2 - y^2 = n$, $ax \equiv b [n]$; |
| ☐ démontrer les critères par 3, 9, 11 ; | ☐ résoudre par les restes ou par encadrement. |

Test d'entrée : par où commencer ?

 15 minutes

 Sans calculatrice

+1 1 point par question

 Réponses sur ta feuille

Avant le cours, fais le point : bloc 1, l'arithmétique du **tronc commun** ; bloc 2, le **chapitre 1** ; bloc 3, le calcul. Aucune question ne demande le cours. Corrigé et orientation : **page 68**.

Bloc 1 · Arithmétique du tronc commun

___ / 4

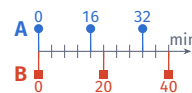
① **Diviseurs et multiples** (a) Quels sont les diviseurs de 75 ? (b) Combien y a-t-il de multiples de 13 entre 200 et 400 ?

② **Divisibilité** (a) Parmi 2, 3, 4, 5 et 9, lesquels divisent 5 148 ?
(b) Pour quels chiffres a , 3 divise-t-il $\overline{4a71}$?

③ **Premier ou pas ?** (a) Parmi 187, 197 et 203, lequel est premier ? Justifier.
(b) Décomposer 2 156 en produit de facteurs premiers.

④ **PGCD et PPCM** (a) de 150 et 180 ?

(b) Les bus A et B (frise, en minutes) partent ensemble à 7 h. Quand repartent-ils ensemble ?



Bloc 2 · Raisonnements (chapitre 1)

___ / 4

⑤ **Disjonction des cas** Montrer que, pour tout $n \in \mathbb{N}$, l'entier $5n^2 + 3n$ est pair (distinguer n pair et n impair).

⑥ **Contraposée** $a, b \in \mathbb{N}$. (a) Écrire la contraposée de « si $ab > 36$, alors $a > 6$ ou $b > 6$ ». (b) La démontrer.

⑦ **Par l'absurde** Packs de 6 ou de 15 bouteilles. (a) Montrer par l'absurde qu'on ne peut pas en avoir 100 exactement. (b) Et 99 ?

⑧ **Récurrence** $u_0 = 1$, $u_{n+1} = 3u_n + 2$ ($n \in \mathbb{N}$).
(a) Montrer par récurrence que $u_n = 2 \times 3^n - 1$.
(b) u_1, u_2, u_3 sont premiers ; et u_4 ?

Bloc 3 · Calcul algébrique et puissances

___ / 4

⑨ **Puissances** (a) Écrire $\frac{6^5 \times 4^3}{9^2 \times 2^7}$ sous la forme $2^a \times 3^b$. (b) Écrire $2^{n+3} - 2^{n+1} + 2^n$ sous la forme $k \times 2^n$ ($n \in \mathbb{N}$).

⑩ **Factoriser** (a) Factoriser $x^2 - 9y^2$. (b) En déduire, avec $2\,491 = 50^2 - 9$, que 2 491 est le produit de deux nombres premiers.

⑪ **Polynômes** (a) Trouver a, b, c réels tels que $2x^2 + 5x + 7 = (x + 2)(ax + b) + c$. (b) Pour quels $n \in \mathbb{N}$ $\frac{2n^2 + 5n + 7}{n + 2}$ est-il entier ?

⑫ **Second degré** (a) Trouver deux nombres de somme 17 et de produit 66.
(b) Résoudre dans $\mathbb{R}$: $x^2 + 2x - 24 \leq 0$.
Combien d'entiers relatifs sont solutions ?

Temps écoulé ?

Pose le crayon, compte tes points bloc par bloc et corrige-toi **page 68**.

Bloc 1

___ / 4

+

Bloc 2

___ / 4

+

Bloc 3

___ / 4

=

Mon score

___ / 12

Partie A • Le cours

Définitions, théorèmes, méthodes, pièges et astuces de concours

1 Divisibilité dans $\mathbb{Z}$

Au tronc commun, tu as travaillé dans $\mathbb{N}$: diviseurs, multiples, nombres premiers, PGCD et PPCM. Ce chapitre étend tout cela à $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ et apporte deux outils très puissants : la **division euclidienne** et les **congruences**. Dans tout le chapitre, les lettres $a, b, c, d, k, m, q, r, u, v, x, y$ désignent des **entiers relatifs**, sauf mention contraire.

Définition : divisibilité

Soit a et b deux entiers relatifs. On dit que a **divise** b , et on note $a \mid b$, lorsqu'il existe un entier relatif k tel que $b = ka$. On dit aussi que a est un **diviseur** de b , que b est un **multiple** de a , ou que b est **divisible** par a . Sinon, on note $a \nmid b$.

Exemples. $-6 \mid 42$, car $42 = (-7) \times (-6)$; $7 \nmid 50$, car $7 \times 7 < 50 < 7 \times 8$; $a \mid 0$ pour tout a (car $0 = 0 \times a$) ; $0 \mid b \iff b = 0$; 1 et -1 divisent tout entier ; a et $-a$ divisent a . Comme $b = ka \iff b = (-k)(-a)$, et que $b = ka$ entraîne $|b| = |k| |a|$: $a \mid b \iff -a \mid b \iff |a| \mid |b|$; on peut toujours se ramener à des entiers naturels.

Propriétés de la divisibilité (a, b, c, d, u, v dans $\mathbb{Z}$)

1. $a \mid a$ (réflexivité).
2. Si $a \mid b$ et $b \mid c$, alors $a \mid c$ (transitivité).
3. Si $a \mid b$ et $a \mid c$, alors $a \mid bu + cv$ pour tous u, v de $\mathbb{Z}$; en particulier $a \mid b + c$ et $a \mid b - c$.
4. Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.
5. Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$, c'est-à-dire $a = b$ ou $a = -b$.
6. Si $a \mid b$, alors $ac \mid bc$; si $a \mid b$ et $c \mid d$, alors $ac \mid bd$; en particulier $a \mid b \Rightarrow a^k \mid b^k$ ($k \in \mathbb{N}$).

Démonstrations. 1. $a = 1 \times a$. 2. $b = ka$ et $c = k'b$ donnent $c = (k'k)a$, avec $k'k \in \mathbb{Z}$. 3. $b = ka$ et $c = k'a$ donnent $bu + cv = (ku + k'v)a$. 4. $b = ka$ avec $k \neq 0$ (car $b \neq 0$), donc $|k| \geq 1$ et $|b| = |k| |a| \geq |a|$. 5. Si $a = 0$, alors $b = 0$ (car 0 ne divise que 0) ; sinon $b \neq 0$ pour la même raison, et la propriété 4 donne $|a| \leq |b|$ et $|b| \leq |a|$. 6. $b = ka$ donne $bc = k(ac)$; $b = ka$ et $d = k'c$ donnent $bd = (kk')(ac)$. $\square$

Définition : ensemble des diviseurs, ensemble des multiples

Pour $n \in \mathbb{Z}$, on note $D(n)$ (ou $\mathcal{D}_n$) l'ensemble des diviseurs de n dans $\mathbb{Z}$, et $n\mathbb{Z} = \{kn ; k \in \mathbb{Z}\}$ l'ensemble des multiples de n .

Si $n \neq 0$, $D(n)$ est **fini** (ses éléments vérifient $|d| \leq |n|$, propriété 4) et **symétrique** : $d \in D(n) \iff -d \in D(n)$. Il suffit donc de chercher les diviseurs positifs, en les associant par paires $d \times \frac{|n|}{d} = |n|$. Par exemple, $18 = 1 \times 18 = 2 \times 9 = 3 \times 6$, donc $D(-18) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$ (12 éléments) ;

$D(1) = \{-1, 1\}$, $D(0) = \mathbb{Z}$. Les multiples de 7 forment $7\mathbb{Z} = \{\dots, -14, -7, 0, 7, 14, \dots\}$, et $a \mid b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}$.

Méthode : Comment trouver les entiers n tels que $A(n) \mid B(n)$

1. Combiner $A(n)$ et $B(n)$ (propriété 3) pour **éliminer** n : écrire $B(n) = A(n)Q(n) + c$, avec $Q(n)$ entier et c constant (division de polynômes, ou combinaison $uB - vA$). 2. En déduire $A(n) \mid B(n) \iff A(n) \mid c$ (justifier les **deux** sens). 3. Écrire $A(n) \in D(c)$ et résoudre chaque petite équation. 4. Conclure par l'ensemble des solutions, et contrôler une valeur.

Exemple : deux équations de divisibilité dans $\mathbb{Z}$

- Les $n \in \mathbb{Z}$ tels que $n - 3 \mid 2n + 7$. On a $2n + 7 = 2(n - 3) + 13$. Si $n - 3 \mid 2n + 7$, alors $n - 3$ divise $(2n + 7) - 2(n - 3) = 13$; réciproquement, si $n - 3 \mid 13$, alors $n - 3$ divise $2(n - 3) + 13 = 2n + 7$. Donc $n - 3 \mid 2n + 7 \iff n - 3 \in D(13) = \{-13, -1, 1, 13\}$: $n \in \{-10, 2, 4, 16\}$ (contrôle : pour $n = 16$, $13 \mid 39$).
- Les $n \in \mathbb{Z}$ tels que $n - 2 \mid n^2 + 3n - 1$. La division donne $n^2 + 3n - 1 = (n - 2)(n + 5) + 9$, et comme ci-dessus $n - 2 \mid n^2 + 3n - 1 \iff n - 2 \mid 9 \iff n - 2 \in \{-9, -3, -1, 1, 3, 9\}$: $n \in \{-7, -1, 1, 3, 5, 11\}$ (contrôle : pour $n = 11$, $9 \mid 153 = 9 \times 17$).

Remarque. Un peu d'histoire. Les livres VII à IX des *Éléments* d'**Euclide** (vers 300 av. J.-C.) contiennent déjà la division, l'algorithme du PGCD, l'infinité des nombres premiers et les nombres parfaits. **Diophante** (III^e siècle) étudie les équations en nombres entiers ; **Fermat** puis **Euler** (XVII^e et XVIII^e siècles) en font une véritable théorie. En 1801, à 24 ans, **Gauss** publie les *Recherches arithmétiques* (*Disquisitiones arithmeticae*), où il invente la notation $a \equiv b$ des congruences (section 4).

2 La division euclidienne

Théorème (division euclidienne dans $\mathbb{N}$)

Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple (q, r) d'entiers naturels tel que $a = bq + r$ et $0 \leq r < b$; q est le **quotient** et r le **reste** de la division euclidienne de a par b .

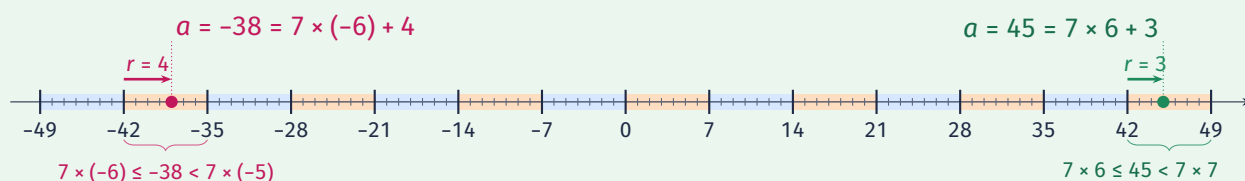
Démonstration. Existence. L'ensemble $A = \{k \in \mathbb{N} ; kb \leq a\}$ contient 0 et il est majoré par a (si $k \in A$, alors $k \leq kb \leq a$, car $b \geq 1$) : c'est une partie finie et non vide de $\mathbb{N}$, qui a donc un plus grand élément q . Posons $r = a - bq$: $r \geq 0$ car $q \in A$; et $q + 1 \notin A$, donc $(q + 1)b > a$, soit $r < b$. **Unicité.** Si $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$, alors $b(q - q') = r' - r$: b divise $r' - r$, et $|r' - r| < b$. Si $r' - r \neq 0$, la propriété 4 de la section 1 donnerait $b \leq |r' - r| < b$: c'est absurde. Donc $r' = r$, puis $bq = bq'$ et $q = q'$ (car $b \neq 0$). $\square$

Théorème (division euclidienne dans $\mathbb{Z}$)

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < |b|$.
Si $b > 0$, $q = E\left(\frac{a}{b}\right)$; si $b < 0$, $q = -E\left(\frac{a}{|b|}\right)$. **Le reste est toujours positif ou nul.**

Démonstration. Existence, cas $b > 0$. Posons $q = E\left(\frac{a}{b}\right) \in \mathbb{Z}$: $q \leq \frac{a}{b} < q + 1$, donc (on multiplie par $b > 0$) $bq \leq a < bq + b$, et $r = a - bq$ vérifie $0 \leq r < b$. **Cas $b < 0$.** On divise a par $|b| = -b > 0$: $a = |b|q' + r$, avec $0 \leq r < |b|$ et $q' = E\left(\frac{a}{|b|}\right)$; donc $a = b(-q') + r$, et $q = -q'$ convient. **Unicité :** mot

pour mot celle du cas de $\mathbb{N}$, avec $|b|$ à la place de b . □



chaque entier a tombe dans **un et un seul** intervalle $[7q, 7q + 7[$: q est le quotient et $r = a - 7q$ le reste

Exemple : les quatre cas de signes, avec $|a| = 125$ et $|b| = 9$ (on part de $125 = 9 \times 13 + 8$)

a, b	division euclidienne	(q, r)	calcul de q
125, 9	$125 = 9 \times 13 + 8$	(13, 8)	$E(13, 8 \dots) = 13$
-125, 9	$-125 = 9 \times (-14) + 1$	(-14, 1)	$E(-13, 8 \dots) = -14$
125, -9	$125 = (-9) \times (-13) + 8$	(-13, 8)	$-E(13, 8 \dots) = -13$
-125, -9	$-125 = (-9) \times 14 + 1$	(14, 1)	$-E(-13, 8 \dots) = 14$

Attention : $-125 = 9 \times (-13) - 8$ est vrai, mais ce **n'est pas** la division euclidienne : le reste -8 est négatif. On « emprunte » un 9 : $-125 = 9 \times (-14) + (9 - 8)$.

À la calculatrice : $\frac{2026}{17} \approx 119,18$, donc $q = 119$ et $r = 2026 - 17 \times 119 = 3$: $2026 = 17 \times 119 + 3$.

Conséquences ($b \in \mathbb{Z}^*$)

- $b \mid a \iff r = 0$.
- Le reste de la division par b prend **exactement** $|b|$ **valeurs** : 0, 1, ..., $|b| - 1$.
- Tout entier est de la forme $2k$ ou $2k+1$; $3k$, $3k+1$ ou $3k+2$ (ou $3k-1$, car $3k+2 = 3(k+1)-1$) ; $4k$, $4k+1$, $4k+2$ ou $4k+3$ ($k \in \mathbb{Z}$).

Démonstration de 1. Si $r = 0$, $a = bq$. Si $a = bk$, alors $(k, 0)$ convient, et par unicité $r = 0$. □

Exemple : a a pour reste 7 dans la division par 9 : restes de $5a + 4$ et de a^2

On écrit $a = 9k + 7$ ($k \in \mathbb{Z}$). $5a + 4 = 45k + 39 = 9(5k + 4) + 3$, avec $0 \leq 3 < 9$: le reste est 3. $a^2 = 81k^2 + 126k + 49 = 9(9k^2 + 14k + 5) + 4$: le reste est 4. **Erreur fréquente :** écrire $5a + 4 = 9 \times 5k + 39$ et répondre « 39 » ; un reste est **strictement inférieur** à $|b|$. (Avec les congruences, section 4 : $a \equiv -2 [9]$, donc $a^2 \equiv 4 [9]$ en une ligne.)

3 Raisonner sur les restes

La division euclidienne par m range les entiers en m familles selon leur reste. Pour démontrer une propriété de **tous** les entiers, il suffit de la démontrer dans chaque famille : c'est un raisonnement par **disjonction des cas** (chapitre 1).

Méthode : Comment raisonner sur les restes

- Choisir le diviseur m** : celui de l'énoncé (« $3 \mid \dots$ » $\rightarrow m = 3$), ou un diviseur qui simplifie (parité $\rightarrow m = 2$; carrés $\rightarrow m = 3, 4$ ou 8).
- Écrire les m cas** : $n = mk, mk + 1, \dots, mk + (m - 1)$, ou de façon symétrique ($3k, 3k \pm 1$; $4k, 4k \pm 1, 4k + 2$) pour alléger les calculs.
- Calculer** l'expression dans chaque cas et l'écrire $mK + s$, avec K entier **explicite** et $0 \leq s < m$.
- Conclure** pour tous les entiers (avec un tableau de restes, section 4).

Parité. n est **pair** si $n = 2k$, **impair** si $n = 2k + 1$ ($k \in \mathbb{Z}$). La somme de deux pairs ou de deux impairs est paire, celle d'un pair et d'un impair est impaire ; un produit est impair si et seulement si tous

ses facteurs le sont ; n^2 a la parité de n . **Deux entiers consécutifs** : l'un des deux est pair, donc $2 \mid n(n+1)$.

Les carrés modulo 3, 4 et 8

Pour tout entier n : 1. n^2 a pour reste 0 ou 1 dans la division par 3 ; 2. n^2 a pour reste 0 ou 1 dans la division par 4 (0 si n est pair, 1 si n est impair) ; 3. n^2 a pour reste 0, 1 ou 4 dans la division par 8, et n impair $\Rightarrow n^2 = 8K + 1$ ($K \in \mathbb{N}$).

Démonstration. 1. $(3k)^2 = 3 \times 3k^2$ et $(3k \pm 1)^2 = 9k^2 \pm 6k + 1 = 3(3k^2 \pm 2k) + 1$. 2. $(2k)^2 = 4k^2$ et $(2k+1)^2 = 4(k^2 + k) + 1$. 3. Si $n = 2k+1$, alors $n^2 = 4k(k+1) + 1$, et $k(k+1) = 2K$ est pair : $n^2 = 8K + 1$. Si $n = 4k$, $n^2 = 8 \times 2k^2$; si $n = 4k+2$, $n^2 = 16k^2 + 16k + 4 = 8(2k^2 + 2k) + 4$. $\square$

Exemple : trois conséquences

1. $3 \mid n^2 + 2 \iff 3 \nmid n$: si $n = 3k$, $n^2 + 2 = 3 \times 3k^2 + 2$ a pour reste 2 ; si $n = 3k \pm 1$, $n^2 + 2 = 3(3k^2 \pm 2k + 1)$.
2. L'équation $x^2 + y^2 = 2031$ n'a **aucune** solution dans $\mathbb{Z}^2$: x^2 et y^2 ont pour reste 0 ou 1 par 4, donc $x^2 + y^2 = 4K + s$ avec $s \in \{0, 1, 2\}$, alors que $2031 = 4 \times 507 + 3$. (Plus généralement, un entier de la forme $4k+3$ n'est **jamais** la somme de deux carrés.)
3. Les nombres 11, 111, 1111, ... (écrits avec $m \geq 2$ chiffres 1) ne sont **jamais des carrés** : ils sont impairs ; $11 = 8 + 3$; et pour $m \geq 3$, $R = 1000N + 111 = 8(125N + 13) + 7$, où N est le nombre formé des $m-3$ premiers chiffres ($N = 0$ si $m = 3$). Leur reste par 8 est 3 ou 7, alors qu'un carré impair a pour reste 1.

Produits d'entiers consécutifs

Pour tout $n \in \mathbb{Z}$: $2 \mid n(n+1)$ et $6 \mid n(n+1)(n+2)$.

Démonstration. Parmi $n, n+1, n+2$, l'un est multiple de 3 (c'est $n, n+2$ ou $n+1$ selon que $n = 3k, 3k+1$ ou $3k+2$) : $P = n(n+1)(n+2) = 3m$. De plus P est pair, car il contient le facteur $n(n+1)$. Ainsi 2 divise $3m$ et $2m$, donc il divise $3m - 2m = m$: $m = 2m'$ et $P = 6m'$. $\square$

Exemple : si n est impair, alors $24 \mid n^3 - n$

$n^3 - n = (n-1)n(n+1)$ est un produit de trois entiers consécutifs : $3 \mid n^3 - n$. Si $n = 2k+1$, alors $(n-1)(n+1) = 2k(2k+2) = 4k(k+1)$, et $k(k+1)$ est pair : $8 \mid (n-1)(n+1)$, donc $8 \mid n^3 - n$. Écrivons $n^3 - n = 8m$: 3 divise $8m$ et $9m$, donc $9m - 8m = m$; d'où $24 \mid n^3 - n$ ($3^3 - 3 = 24$, $5^3 - 5 = 120$, $7^3 - 7 = 336 = 24 \times 14$). Pour n pair, c'est faux : $2^3 - 2 = 6$.

4

Congruence modulo n

Dans toute la suite, n est un entier naturel tel que $n \geq 2$.

Définition : congruence modulo n (Gauss, 1801)

On dit que a est **congru à b modulo n** , et on note $a \equiv b [n]$, lorsque n divise $a-b$, c'est-à-dire lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Exemples. $38 \equiv 3 [7]$ ($38 - 3 = 35$) ; $-38 \equiv 4 [7]$ ($-38 - 4 = -42$) ; $10 \equiv 1 [9]$; $10 \equiv -1 [11]$; $99 \equiv -1 [100]$; $2026 \equiv 3 [7]$ ($2023 = 7 \times 17^2$) ; $a \equiv 0 [n] \iff n \mid a$; a est pair $\iff a \equiv 0 [2]$.

Théorème (congruence et reste)

$a \equiv b [n] \iff a$ et b ont **le même reste** dans la division euclidienne par n . En particulier, si r est le reste de a par n , alors $a \equiv r [n]$, et **tout entier est congru modulo n à un et un seul des entiers $0, 1, \dots, n-1$.**

Démonstration. Écrivons $a = nq + r$ et $b = nq' + r'$, avec $0 \leq r < n$ et $0 \leq r' < n$: $a - b = n(q - q') + (r - r')$.
 $(\Leftarrow)$ Si $r = r'$, alors $a - b = n(q - q')$. $(\Rightarrow)$ Si $n \mid a - b$, alors n divise $(a - b) - n(q - q') = r - r'$, avec $|r - r'| < n$: donc $r - r' = 0$ (section 1, propriété 4). Enfin, si $a \equiv s [n]$ avec $0 \leq s < n$, le reste de s par n est s lui-même, donc $s = r$. $\square$

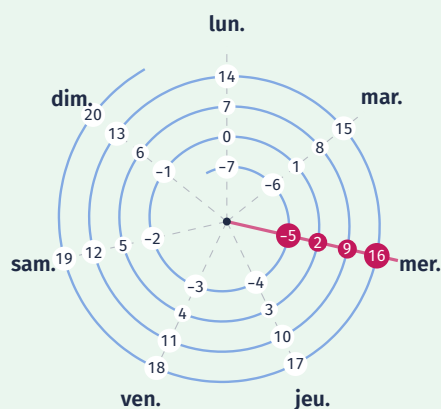
Propriétés des congruences (a, b, c, d, m dans $\mathbb{Z}$, $k \in \mathbb{N}$)

- $a \equiv a [n]$; si $a \equiv b [n]$, alors $b \equiv a [n]$; si $a \equiv b [n]$ et $b \equiv c [n]$, alors $a \equiv c [n]$.
- Compatibilité.** Si $a \equiv b [n]$ et $c \equiv d [n]$, alors $a + c \equiv b + d [n]$, $a - c \equiv b - d [n]$ et $ac \equiv bd [n]$.
- Puissances.** Si $a \equiv b [n]$, alors $a^k \equiv b^k [n]$ pour tout $k \in \mathbb{N}$, et $ma \equiv mb [n]$.
- Si $a \equiv b [n]$ et si $d \geq 2$ divise n , alors $a \equiv b [d]$.

Démonstrations. 1. $a - a = 0$; $b - a = -(a - b)$; $a - c = (a - b) + (b - c)$ (section 1, propriété 3). 2. $(a + c) - (b + d) = (a - b) + (c - d)$; de même pour la différence ; et $ac - bd = a(c - d) + d(a - b)$ est une combinaison de deux multiples de n . 3. Par récurrence sur k : $a^0 = b^0 = 1$; si $a^k \equiv b^k [n]$, alors $a^{k+1} = a^k \times a \equiv b^k \times b = b^{k+1} [n]$ par 2. Puis 2 avec $c = d = m$ donne $ma \equiv mb [n]$. 4. $d \mid n$ et $n \mid a - b$ (transitivité). $\square$

En pratique : dans une somme, un produit ou une puissance, on peut **remplacer chaque nombre par un nombre qui lui est congru** : son reste, ou un petit entier négatif. Par exemple, modulo 7 : $2026 \equiv 3$, $2027 \equiv 4$ et $2028 \equiv 5 \equiv -2$, donc $2026 \times 2027 + 2028^2 \equiv 3 \times 4 + (-2)^2 = 16 \equiv 2 [7]$, sans aucune grande multiplication.

L'image de l'horloge. Enroulons les entiers sur une spirale à 7 rayons (figure) : deux entiers sont congrus modulo 7 si et seulement s'ils sont **sur le même rayon**. Si l'on numérote 0 le lundi, 1 le mardi, etc., le jour de la semaine est donné par le rayon : comme $1000 = 7 \times 142 + 6$, $1000 \equiv 6 \equiv -1 [7]$, et 1000 jours après un lundi, on est un dimanche.



rayon des entiers $\equiv 2 [7]$: ..., -5, 2, 9, 16, ...

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

table de multiplication modulo 7

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

table de multiplication modulo 8

Lire les tables (case (i, j) : le reste de ij). **Modulo 7** : chaque ligne, sauf celle de 0, contient **une fois et une seule** chaque reste ; si $a \not\equiv 0 [7]$, l'équation $ax \equiv b [7]$ a donc une unique solution modulo 7 (section 11). **Modulo 8** : la diagonale (en jaune) donne les **carrés** : 0, 1, 4 seulement (section 3) ; et $2 \times 4 \equiv 4 \times 6 \equiv 0 [8]$ (en rouge) : un produit peut être congru à 0 sans qu'aucun facteur le soit

(section 13).

Exemple : un tableau de restes : pour quels entiers n a-t-on $6 \mid n^2 + 2n + 3$?

Modulo 6, n est congru à l'un des restes $r \in \{0, \dots, 5\}$, et alors $n^2 + 2n + 3 \equiv r^2 + 2r + 3 \pmod{6}$ (compatibilité). On remplit le tableau ci-contre, puis on lit :

$$6 \mid n^2 + 2n + 3 \iff n \equiv 1 \text{ ou } n \equiv 3 \pmod{6}$$

(contrôle : $n = 7$ donne $66 = 6 \times 11$).

$n \equiv \dots \pmod{6}$	0	1	2	3	4	5
$n^2 \equiv$	0	1	4	3	4	1
$2n \equiv$	0	2	4	0	2	4
$n^2 + 2n + 3 \equiv$	3	0	5	0	3	2

5

Calculer avec les congruences

Méthode : Comment calculer le reste d'une grande puissance a^N modulo n

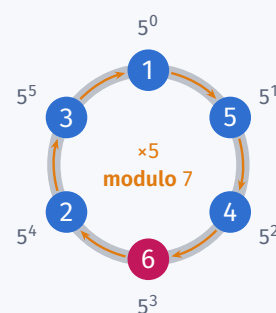
1. Remplacer a par son reste, ou par un petit entier qui lui est congru (éventuellement négatif). 2. Calculer les puissances successives modulo n (chacune à partir de la précédente) jusqu'à trouver un exposant $k \geq 1$ tel que $a^k \equiv 1 \pmod{n}$, ou $a^k \equiv -1 \pmod{n}$. 3. Diviser l'exposant par k : $N = kq + s$ avec $0 \leq s < k$, d'où $a^N = (a^k)^q \times a^s \equiv 1^q \times a^s = a^s \pmod{n}$ (ou $(-1)^q a^s$). 4. Conclure par un reste compris entre 0 et $n - 1$.

Exemple : les puissances de 5 modulo 7 : un cycle de longueur 6

$5^0 = 1$, $5^1 = 5$, $5^2 = 25 \equiv 4$, $5^3 \equiv 4 \times 5 = 20 \equiv 6$, $5^4 \equiv 6 \times 5 \equiv 2$, $5^5 \equiv 2 \times 5 \equiv 3$, $5^6 \equiv 3 \times 5 \equiv 1 \pmod{7}$: on revient à 1. Comme $5^{k+6} = 5^k \times 5^6 \equiv 5^k \pmod{7}$, la suite des restes est **périodique de période 6** : le reste de 5^N ne dépend que du reste de N par 6.

1. $2026 = 6 \times 337 + 4$, donc $5^{2026} = (5^6)^{337} \times 5^4 \equiv 1 \times 2 \pmod{7}$: le reste est $\boxed{2}$.

2. Pour quels $n \in \mathbb{N}$ a-t-on $7 \mid 5^n + 1$? Il faut $5^n \equiv 6 \pmod{7}$, et 6 n'apparaît qu'en position 3 du cycle : $7 \mid 5^n + 1 \iff n \equiv 3 \pmod{6}$ (contrôle : $5^3 + 1 = 126 = 7 \times 18$).

**Exemple : le raccourci $a^k \equiv -1$: 3^{2026} modulo 14, puis 6^{2026} modulo 13**

$3^3 = 27 = 2 \times 14 - 1$, donc $3^3 \equiv -1 \pmod{14}$; comme $2026 = 3 \times 675 + 1$: $3^{2026} = (3^3)^{675} \times 3 \equiv (-1)^{675} \times 3 = -3 \equiv \boxed{11} \pmod{14}$.

$6^2 = 36 \equiv -3 \pmod{13}$, donc $6^6 = (6^2)^3 \equiv (-3)^3 = -27 \equiv -1 \pmod{13}$; comme $2026 = 6 \times 337 + 4$ et $6^4 \equiv (-3)^2 = 9$: $6^{2026} \equiv (-1)^{337} \times 9 = -9 \equiv \boxed{4} \pmod{13}$.

Une divisibilité pour tout n , sans récurrence : $25 \equiv 2 \pmod{23}$, donc $5^{2n} = 25^n \equiv 2^n \pmod{23}$: $23 \mid 5^{2n} - 2^n$ pour tout $n \in \mathbb{N}$ ($25^2 - 2^2 = 621 = 23 \times 27$).

Le dernier chiffre. Le chiffre des unités d'un entier naturel N est son reste modulo 10, et il ne dépend que du dernier chiffre c de N (tableau) : **un carré ne se termine jamais par 2, 3, 7 ou 8**. Les derniers chiffres des puissances sont périodiques, de période 1, 2 ou 4 : $2 \rightarrow 4 \rightarrow 8 \rightarrow 6$, $3 \rightarrow 9 \rightarrow 7 \rightarrow 1$, $7 \rightarrow 9 \rightarrow 3 \rightarrow 1$, $8 \rightarrow 4 \rightarrow 2 \rightarrow 6$, $4 \rightarrow 6$, $9 \rightarrow 1$; ainsi $2^{100} + 3^{100}$ se termine par $6 + 1 = 7$ ($100 \equiv 0 \pmod{4}$).

dernier chiffre c de N	0	1	2	3	4	5	6	7	8	9
dernier chiffre de N^2	0	1	4	9	6	5	6	9	4	1
dernier chiffre de N^4	0	1	6	1	6	5	6	1	6	1

Théorème (critères de divisibilité)

Soit $N = \overline{a_m \dots a_1 a_0} = a_m 10^m + \dots + a_1 \times 10 + a_0$ un entier naturel écrit en base 10 (chiffres $a_i \in \{0, \dots, 9\}$), et $S = a_0 + a_1 + \dots + a_m$ la somme de ses chiffres.

1. $N \equiv a_0 [10]$: $2 \mid N \iff a_0$ est pair ; $5 \mid N \iff a_0 \in \{0, 5\}$. 2. $4 \mid N \iff 4 \mid \overline{a_1 a_0}$; $8 \mid N \iff 8 \mid \overline{a_2 a_1 a_0}$.

3. $N \equiv S [9]$, donc $9 \mid N \iff 9 \mid S$ et $3 \mid N \iff 3 \mid S$.

4. $N \equiv a_0 - a_1 + a_2 - \dots + (-1)^m a_m [11]$, donc $11 \mid N \iff 11$ divise cette somme alternée.

Démonstration. 1. $N = 10 \times \overline{a_m \dots a_1} + a_0 \equiv a_0 [10]$, puis on passe modulo 2 et 5, qui divisent 10 (propriété 4 des congruences). 2. $N = 100 \times \overline{a_m \dots a_2} + \overline{a_1 a_0}$ et $100 \equiv 0 [4]$; de même $1000 \equiv 0 [8]$. 3. $10 \equiv 1 [9]$, donc $10^i \equiv 1^i = 1 [9]$ pour tout i , et $N \equiv a_m + \dots + a_1 + a_0 [9]$; enfin $3 \mid 9$. 4. $10 \equiv -1 [11]$, donc $10^i \equiv (-1)^i [11]$. $\square$

Exemple : $N = 6\,237\,504$, puis des chiffres inconnus

$a_0 = 4$: N est pair, non multiple de 5. $\overline{04} = 4$ et $\overline{504} = 8 \times 63$: $4 \mid N$ et $8 \mid N$. $S = 6 + 2 + 3 + 7 + 5 + 0 + 4 = 27$: $9 \mid N$ (donc $3 \mid N$). Somme alternée, en partant des unités : $4 - 0 + 5 - 7 + 3 - 2 + 6 = 9$: $N \equiv 9 [11]$ et $11 \nmid N$. (Section 10 : $8 \mid N$ et $9 \mid N$ donnent $72 \mid N$; en effet $N = 72 \times 86\,632$.)

Chiffres inconnus. Cherchons les chiffres x et y tels que $M = \overline{2x73y}$ soit divisible par 4 et par 9. $4 \mid \overline{3y} \iff y \in \{2, 6\}$ (seuls 32 et 36 conviennent entre 30 et 39) ; $9 \mid 2 + x + 7 + 3 + y = 12 + x + y$, avec $0 \leq x + y \leq 18$, impose $x + y \in \{6, 15\}$. D'où $(x, y) \in \{(4, 2), (0, 6), (9, 6)\}$: $M \in \{24\,732, 20\,736, 29\,736\}$.

6

Les nombres premiers**Définition : nombre premier, nombre composé**

Un entier naturel p est **premier** lorsque $p \geq 2$ et que ses seuls diviseurs positifs sont 1 et p (dans $\mathbb{Z}$: $D(p) = \{-p, -1, 1, p\}$). Un entier $n \geq 2$ qui n'est pas premier est dit **composé** : il s'écrit $n = ab$ avec $1 < a < n$ et $1 < b < n$.

2, 3, 5, 7, 11, 13, ... sont premiers ; 1 **n'est pas premier** (il n'a qu'un diviseur positif) ; 2 est le seul nombre premier pair.

Théorème (existence d'un diviseur premier)

Tout entier $n \geq 2$ admet au moins un diviseur premier : son **plus petit diviseur** $p > 1$ est **premier**. De plus, si n est composé, ce plus petit diviseur premier vérifie $p^2 \leq n$.

Démonstration. L'ensemble des diviseurs $d > 1$ de n est une partie non vide de $\mathbb{N}$ (il contient n) : il a un plus petit élément p . Si p n'était pas premier, il aurait un diviseur d' tel que $1 < d' < p$; par transitivité, $d' \mid n$, ce qui contredit le choix de p . Si n est composé, $n \neq p$, donc $n = pm$ avec $m > 1$; m est un diviseur de n strictement supérieur à 1, donc $m \geq p$, et $n = pm \geq p^2$. $\square$ (Autre preuve : récurrence forte, chapitre 1.)

Méthode : Comment savoir si n est premier : le critère $\sqrt{n}$

Par contraposée du théorème : **si aucun nombre premier p tel que $p^2 \leq n$ ne divise n , alors n est premier.** On essaie donc 2, 3, 5, 7, 11, ... (critères de la section 5), jusqu'au plus grand nombre premier $p \leq \sqrt{n}$, et l'on s'arrête dès qu'une division tombe juste : n est alors composé.

Exemples. $21^2 = 441 < 457 < 484 = 22^2$, et aucun des nombres premiers 2, 3, 5, 7, 11, 13, 17, 19 ne divise 457 (restes 1, 1, 2, 2, 6, 2, 15, 1) : **457 est premier.** Pour 493 ($22^2 < 493 < 23^2$), les essais 2, 3, 5, 7, 11, 13 échouent, mais $493 = 17 \times 29$: **composé.**

Le crible d'Ératosthène (III^e siècle av. J.-C.). On écrit les entiers de 2 à 120 ; on garde 2 et on barre ses multiples ; le premier nombre non barré, 3, est premier : on le garde et on barre ses multiples ; puis on recommence avec 5 et 7. On peut s'arrêter là, car $11^2 = 121 > 120$: un nombre composé $n \leq 120$ a un facteur premier $p \leq \sqrt{n} < 11$, donc il a été barré. Il reste les 30 **nombres premiers** inférieurs à 120 (en bleu) ; chaque nombre composé est barré dans la couleur de son plus petit facteur premier : 2, 3, 5 ou 7.

$12k+1$					$12k+5$					$12k+7$					$12k+11$				
1	2	3	4	5	6	7	8	9	10	11	12								
13	14	15	16	17	18	19	20	21	22	23	24								
25	26	27	28	29	30	31	32	33	34	35	36								
37	38	39	40	41	42	43	44	45	46	47	48								
49	50	51	52	53	54	55	56	57	58	59	60								
61	62	63	64	65	66	67	68	69	70	71	72								
73	74	75	76	77	78	79	80	81	82	83	84								
85	86	87	88	89	90	91	92	93	94	95	96								
97	98	99	100	101	102	103	104	105	106	107	108								
109	110	111	112	113	114	115	116	117	118	119	120								

colonnes vertes : restes 1, 5, 7, 11 modulo 12

Les nombres premiers $p \geq 5$ (ce que montre le crible)

Tout nombre premier $p \geq 5$ s'écrit $6k+1$ ou $6k-1$ ($k \in \mathbb{N}^*$) : $p \equiv \pm 1 [6]$. (Dans le crible en 12 colonnes, les nombres premiers $p \geq 5$ sont tous dans les colonnes vertes.)

Démonstration. Modulo 6, p est congru à 0, ± 1 , ± 2 ou 3. Si $p \equiv 0$ ou $p \equiv \pm 2 [6]$, p est pair ; si $p \equiv 3 [6]$, $3 \mid p$; dans ces cas $p = 2$ ou $p = 3$, exclus. $\square$ La réciproque est fautive : $25 = 6 \times 4 + 1$ et $35 = 6 \times 6 - 1$.

Théorème (Euclide : il existe une infinité de nombres premiers)

Pour tout entier $n \geq 1$, il existe un nombre premier $p > n$: l'ensemble des nombres premiers n'est pas majoré, il est **infini**.

Démonstration. L'entier $N = n! + 1 \geq 2$ admet un diviseur premier p (théorème précédent). Si l'on avait $p \leq n$, p serait l'un des facteurs de $n! = 1 \times 2 \times \dots \times n$, donc $p \mid n!$; comme $p \mid N$, il diviserait $N - n! = 1$: c'est impossible, car $p \geq 2$. Donc $p > n$. $\square$

Exemples : $4! + 1 = 25 = 5^2$ (et $5 > 4$) ; $5! + 1 = 121 = 11^2$; $6! + 1 = 721 = 7 \times 103$. Euclide (*Éléments*, livre IX) utilisait le nombre $p_1 p_2 \dots p_k + 1$, construit à partir de nombres premiers donnés $p_1, \dots, p_k$.

Lemme (admis cette année, démontré en 2^e Bac)

Soit p un nombre premier et a, b des entiers. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$. Par récurrence : si p divise un produit $a_1 a_2 \dots a_k$, il divise l'un des facteurs ; si $p \mid a^k$, alors $p \mid a$; si p divise un produit de nombres premiers, il est égal à l'un d'eux.

Exemple. Si $7 \mid n^2$, alors $7 \mid n$, donc $n = 7m$ et $49 \mid n^2$. **Attention :** le lemme est faux si p n'est pas premier : $6 \mid 4 \times 9$, mais $6 \nmid 4$ et $6 \nmid 9$.

7

Décomposition en facteurs premiers

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ s'écrit comme un **produit de nombres premiers** :

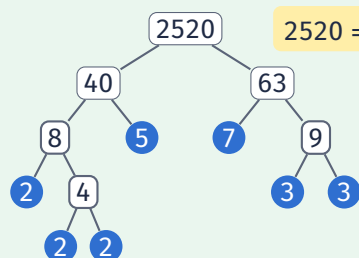
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad p_1 < p_2 < \cdots < p_k \text{ premiers}, \quad \alpha_1, \dots, \alpha_k \in \mathbb{N}^*,$$

et cette écriture, la **décomposition en facteurs premiers** de n , est **unique** (unicité admise cette année). Pour $n \in \mathbb{Z}$ tel que $|n| \geq 2$, on écrit $n = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

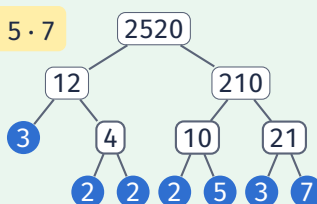
Démonstration de l'existence (par l'absurde, avec le plus petit contre-exemple). Supposons non vide l'ensemble E des entiers $n \geq 2$ qui **ne** sont **pas** des produits de nombres premiers ; il a un plus petit élément n . Un nombre premier est un produit (d'un seul facteur), donc n est composé : $n = ab$, avec $2 \leq a < n$ et $2 \leq b < n$. Par minimalité de n , $a \notin E$ et $b \notin E$: a et b sont des produits de nombres premiers, donc $n = ab$ aussi, ce qui contredit $n \in E$. $\square$

Méthode : Comment décomposer un entier

Divisions successives : on divise par 2 tant que c'est possible, puis par 3, 5, 7, ... (critères de la section 5) ; on s'arrête quand le quotient vaut 1, ou quand il est premier (aucun diviseur premier $\leq$ sa racine carrée). **Arbre** : on casse n en un produit **quelconque** de deux facteurs, puis chaque facteur, jusqu'aux feuilles, qui sont premières ; l'unicité garantit que **tous les arbres ont les mêmes feuilles**.

arbre 1 : $2520 = 40 \times 63$

$$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

arbre 2 : $2520 = 12 \times 210$

2520	2
1260	2
630	2
315	3
105	3
35	5
7	7
1	

divisions successives

Diviseurs, nombre et somme des diviseurs

Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. 1. Les diviseurs positifs de n sont les entiers $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout i .

2. n a donc $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ diviseurs positifs (deux fois plus dans $\mathbb{Z}$).

3. Leur somme est $\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k}) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \times \cdots \times \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}$.

Démonstration. 1. Un tel d divise n , car $n = d \times p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k - \beta_k}$. Réciproquement, si $n = dm$ avec $d \geq 1$ et $m \geq 1$: tout facteur premier de d divise n , donc (lemme de la section 6) c'est l'un des p_i , et de même pour m ; en écrivant $d = \prod p_i^{\beta_i}$ et $m = \prod p_i^{\gamma_i}$, le produit $\prod p_i^{\beta_i + \gamma_i}$ est une décomposition de n , et l'unicité donne $\beta_i + \gamma_i = \alpha_i$, donc $\beta_i \leq \alpha_i$. 2. Chaque β_i peut prendre $\alpha_i + 1$

valeurs, indépendamment des autres, et deux choix différents donnent deux diviseurs différents (unicité). 3. En développant le produit, on obtient une fois et une seule chaque $p_1^{\beta_1} \dots p_k^{\beta_k}$; enfin $1 + p + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$ (somme géométrique). $\square$

Exemple : les diviseurs de $108 = 2^2 \cdot 3^3$, puis ceux de 2520

$\times$	1	3	9	27
1	1	3	9	27
2	2	6	18	54
4	4	12	36	108

On croise les diviseurs 1, 2, 4 de 2^2 et 1, 3, 9, 27 de 3^3 : $(2 + 1)(3 + 1) = 12$ diviseurs positifs, de somme $(1 + 2 + 4)(1 + 3 + 9 + 27) = 7 \times 40 = 280$.
 $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ a $(3 + 1)(2 + 1)(1 + 1)(1 + 1) = 48$ diviseurs positifs, de somme $15 \times 13 \times 6 \times 8 = 9360$.

Carrés parfaits

Un entier $n \geq 2$ est un **carré parfait** ($n = m^2$, $m \in \mathbb{N}$) $\iff$ tous les exposants α_i de sa décomposition sont **pairs** $\iff$ n a un nombre **impair** de diviseurs positifs. De même, n est un cube $\iff$ tous les α_i sont multiples de 3.

Démonstration. Si $m = \prod p_i^{\gamma_i}$, alors $m^2 = \prod p_i^{2\gamma_i}$, et l'unicité donne $\alpha_i = 2\gamma_i$; réciproquement, si chaque $\alpha_i = 2\gamma_i$, alors $n = \left(\prod p_i^{\gamma_i}\right)^2$. Enfin, le produit $\prod(\alpha_i + 1)$ est impair $\iff$ chaque $\alpha_i + 1$ est impair $\iff$ chaque α_i est pair. $\square$

Exemples. 108 n'est pas un carré (exposant 3) et a 12 diviseurs ; $3600 = 2^4 \cdot 3^2 \cdot 5^2 = 60^2$ a $5 \times 3 \times 3 = 45$ diviseurs. Plus petit entier $k \geq 1$ tel que $2520k$ soit un **cube** : il faut compléter chaque exposant jusqu'à un multiple de 3, donc $k = 3 \cdot 5^2 \cdot 7^2 = 3675$, et $2520 \times 3675 = 2^3 \cdot 3^3 \cdot 5^3 \cdot 7^3 = 210^3 = 9\,261\,000$.

8

Le PGCD

Définition : plus grand commun diviseur

Soit a et b deux entiers **non tous deux nuls**. L'ensemble $D(a) \cap D(b)$ de leurs diviseurs communs contient 1 et il est fini (si $a \neq 0$, ses éléments vérifient $|d| \leq |a|$) : il a un plus grand élément, le **PGCD** de a et b , noté $a \wedge b$ (ou $\text{PGCD}(a, b)$).

Premières propriétés. 1. $a \wedge b = b \wedge a = |a| \wedge |b| \geq 1$ (car $D(-a) = D(a)$). 2. $a \wedge 0 = |a|$ si $a \neq 0$ (car $D(0) = \mathbb{Z}$) ; $a \wedge 1 = 1$. 3. Si $b \neq 0$: $b \mid a \iff a \wedge b = |b|$ (tout diviseur de b est au plus égal à $|b|$). 4. $a \wedge b$ divise a et b , donc **toute combinaison** $au + bv$ ($u, v \in \mathbb{Z}$).

Lemme (le cœur de l'algorithme d'Euclide)

Si $a = bq + r$ (avec a, b, q, r dans $\mathbb{Z}$, $b \neq 0$), alors $D(a) \cap D(b) = D(b) \cap D(r)$, et donc $a \wedge b = b \wedge r$. (r n'est pas forcément le reste : le lemme vaut pour **tout** entier q .)

Démonstration (double inclusion). Si $d \mid a$ et $d \mid b$, alors d divise $a - bq = r$; si $d \mid b$ et $d \mid r$, alors d divise $bq + r = a$. Les deux ensembles sont égaux, donc ils ont le même plus grand élément. $\square$

Théorème (algorithme d'Euclide)

Soit $a \geq b > 0$. On pose $r_0 = a$, $r_1 = b$ et, tant que $r_k \neq 0$, on note r_{k+1} le reste de la division de r_{k-1} par r_k . Les restes décroissent strictement : on atteint un reste nul $r_{m+1} = 0$, et le **PGCD**

est le dernier reste non nul : $a \wedge b = r_m$. De plus $D(a) \cap D(b) = D(a \wedge b)$: les diviseurs communs à a et b sont exactement les diviseurs de $a \wedge b$.

Démonstration. Une suite strictement décroissante d'entiers naturels ne peut pas être infinie (elle prend au plus $b+1$ valeurs entre b et 0). Par le lemme, $D(r_0) \cap D(r_1) = D(r_1) \cap D(r_2) = \dots = D(r_m) \cap D(0) = D(r_m)$, car $D(0) = \mathbb{Z}$; le plus grand élément de $D(r_m)$ est r_m . $\square$

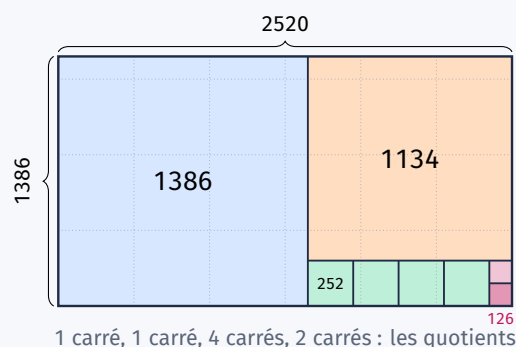
Exemple : le fil rouge : $2520 \wedge 1386$ par l'algorithme d'Euclide

r_{k-1}	r_k	q_k	division
2520	1386	1	$2520 = 1386 \times 1 + 1134$
1386	1134	1	$1386 = 1134 \times 1 + 252$
1134	252	4	$1134 = 252 \times 4 + 126$
252	126	2	$252 = 126 \times 2 + 0$

Le dernier reste non nul est 126 :

$2520 \wedge 1386 = 126$. Les diviseurs communs à 2520 et 1386 sont les 24 diviseurs de $126 = 2 \cdot 3^2 \cdot 7$ (12 positifs).

En carrés : dans un rectangle 2520×1386 , on retire le plus grand carré possible, autant de fois que possible (le quotient), et l'on recommence dans ce qui reste : le dernier carré, de côté 126, **pave tout le rectangle** (pointillés).



Propriétés (homogénéité, décomposition)

- Pour $k \in \mathbb{Z}^*$: $(ka) \wedge (kb) = |k| (a \wedge b)$.
- Si $|a| = \prod p_i^{\alpha_i}$ et $|b| = \prod p_i^{\beta_i}$ (mêmes nombres premiers p_i , exposants α_i, β_i dans $\mathbb{N}$, éventuellement nuls), alors $a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}$: on garde les facteurs **communs**, avec le **plus petit** exposant.

Démonstrations. 1. Pour $k > 0$ et $a \geq b > 0$ (les autres cas s'y ramènent) : si $r_{i-1} = r_i q_i + r_{i+1}$ avec $0 \leq r_{i+1} < r_i$, alors $kr_{i-1} = (kr_i)q_i + kr_{i+1}$ avec $0 \leq kr_{i+1} < kr_i$; l'algorithme pour ka et kb a pour restes les kr_i , et se termine par $kr_m = k(a \wedge b)$. 2. D'après la section 7, $d = \prod p_i^{\delta_i}$ divise a et $b \iff \delta_i \leq \alpha_i$ et $\delta_i \leq \beta_i$ pour tout $i \iff \delta_i \leq \min(\alpha_i, \beta_i)$; le plus grand est obtenu pour $\delta_i = \min(\alpha_i, \beta_i)$. $\square$

Fil rouge : $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ et $1386 = 2 \cdot 3^2 \cdot 7 \cdot 11$, donc $2520 \wedge 1386 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 126$: on retrouve Euclide. De même $12\,600 \wedge 6930 = 5 \times (2520 \wedge 1386) = 630$.

Méthode : Comment calculer un PGCD

- Petits nombres :** lister les diviseurs.
- Grands nombres :** l'algorithme d'Euclide (rapide, sans décomposer).
- Décompositions connues :** les plus petits exposants.
- Expressions en n :** appliquer le lemme $a \wedge b = b \wedge (a - bq)$ avec un q bien choisi, ou combiner pour éliminer n (le PGCD divise toute combinaison), jusqu'à une constante c ; le PGCD divise c , puis on cherche pour quels n chaque diviseur de c est atteint.

Exemple : $d_n = (2n + 5) \wedge (3n + 1)$ pour $n \in \mathbb{Z}$

Lemme, deux fois : $3n+1 = (2n+5) \times 1 + (n-4)$, puis $2n+5 = (n-4) \times 2 + 13$; donc $d_n = (2n+5) \wedge (n-4) = (n-4) \wedge 13$. Comme 13 est premier, $d_n \in \{1, 13\}$, et $d_n = 13 \iff 13 \mid n-4 \iff n \equiv 4 \pmod{13}$.

Contrôles : $n = 17$ donne $39 \wedge 52 = 13$; $n = 5$ donne $15 \wedge 16 = 1$. (Par combinaison : $3(2n+5) - 2(3n+1) = 13$, donc $d_n \mid 13$.)

9

Le PPCM

Définition : plus petit commun multiple

Soit a et b deux entiers **non nuls**. L'ensemble de leurs multiples communs **strictement positifs** contient $|ab|$; il a donc un plus petit élément : le **PPCM** de a et b , noté $a \vee b$ (ou $\text{PPCM}(a, b)$).

Par exemple $6 \vee 9 = 18$; $a \vee b = b \vee a = |a| \vee |b|$; $a \mid b \iff a \vee b = |b|$; $a \vee 1 = |a|$.

Théorème (les multiples communs)

Les multiples communs à a et b sont exactement les multiples de $a \vee b$: $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Démonstration. Posons $\mu = a \vee b$. Un multiple de μ est multiple de a et de b (transitivité). Réciproquement, soit m un multiple commun ; divisons-le par μ : $m = \mu q + r$, avec $0 \leq r < \mu$. Alors $r = m - \mu q$ est un multiple commun de a et b (section 1, propriété 3), et $0 \leq r < \mu$: par définition de μ , r ne peut pas être strictement positif, donc $r = 0$ et $\mu \mid m$. $\square$

Théorème (PPCM, décomposition et PGCD)

1. Avec les notations de la section 8 : $a \vee b = \prod p_i^{\max(\alpha_i, \beta_i)}$ (tous les facteurs, avec le **plus grand** exposant).
2. $(a \wedge b) \times (a \vee b) = |ab|$.
3. Pour $k \in \mathbb{Z}^*$: $(ka) \vee (kb) = |k| (a \vee b)$.

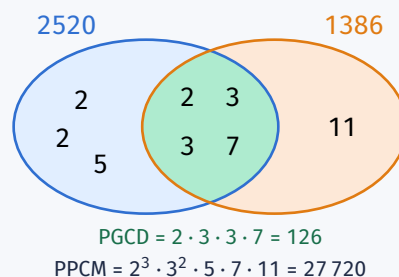
Démonstration. 1. D'après la section 7, un entier $m \geq 1$ est multiple de a et de $b \iff$ dans sa décomposition, chaque p_i figure avec un exposant $\mu_i \geq \alpha_i$ et $\mu_i \geq \beta_i$; le plus petit est $\prod p_i^{\max(\alpha_i, \beta_i)}$.

2. Pour deux réels, $\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta$, donc $(a \wedge b)(a \vee b) = \prod p_i^{\alpha_i + \beta_i} = |a| \times |b|$. 3. Par 2 et l'homogénéité du PGCD : $(ka) \vee (kb) = \frac{k^2 |ab|}{|k| (a \wedge b)} = |k| (a \vee b)$. $\square$

Exemple : le fil rouge et le diagramme des facteurs premiers

$2520 \vee 1386 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27\,720$ (ou $\frac{2520 \times 1386}{126} = 2520 \times 11$). Contrôle : $126 \times 27\,720 = 3\,492\,720 = 2520 \times 1386$. **Dénominateur commun** : c'est le PPCM des dénominateurs. $180 = 2^2 \cdot 3^2 \cdot 5$ et $168 = 2^3 \cdot 3 \cdot 7$, donc $180 \vee 168 = 2520$ et $\frac{7}{180} + \frac{11}{168} = \frac{7 \times 14 + 11 \times 15}{2520} = \frac{263}{2520}$ (irréductible : 263 est premier). Et 2520 est le PPCM de 1, 2, ..., 10 ($2^3, 3^2, 5, 7$).

Lecture du diagramme : on place les facteurs premiers (répétés) de chaque nombre dans son disque ; les facteurs communs vont dans l'intersection. Le PGCD est le produit de l'**intersection**, le PPCM celui de la **réunion** ; et $\text{PGCD} \times \text{PPCM}$ compte chaque facteur autant de fois que $a \times b$.



10

Nombres premiers entre eux

Définition : entiers premiers entre eux

a et b sont **premiers entre eux** lorsque $a \wedge b = 1$: leurs seuls diviseurs communs sont 1 et -1 .

Exemples. $n \wedge (n + 1) = 1$ (un diviseur commun divise $(n + 1) - n = 1$) ; $n \wedge (n^2 + 1) = 1$ (il divise $(n^2 + 1) - n \times n$) ; deux nombres premiers distincts sont premiers entre eux ; si p est premier, $p \wedge a = 1 \iff p \nmid a$ (car $p \wedge a$ divise p , il vaut 1 ou p). **Attention :** « premiers entre eux » ne veut pas dire « premiers » : $8 \wedge 15 = 1$.

Caractérisation

$a \wedge b = 1 \iff a$ et b n'ont **aucun facteur premier commun** $\iff a \vee b = |ab|$.

Démonstration. $\prod p_i^{\min(\alpha_i, \beta_i)} = 1 \iff$ chaque $\min(\alpha_i, \beta_i)$ est nul ; puis $(a \wedge b)(a \vee b) = |ab|$. $\square$

Théorème

Si $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors $ab \mid c$. Plus généralement, si des entiers **deux à deux** premiers entre eux divisent c , leur produit divise c .

Démonstration (par la décomposition ; si $c = 0$, c'est évident). Écrivons $|a| = \prod p_i^{\alpha_i}$, $|b| = \prod p_i^{\beta_i}$, $|c| = \prod p_i^{\gamma_i}$, avec les mêmes p_i et des exposants éventuellement nuls. Par la section 7, $\alpha_i \leq \gamma_i$ et $\beta_i \leq \gamma_i$. Comme a et b n'ont pas de facteur premier commun, pour chaque i , $\alpha_i = 0$ ou $\beta_i = 0$; donc $\alpha_i + \beta_i = \max(\alpha_i, \beta_i) \leq \gamma_i$, et $|ab| = \prod p_i^{\alpha_i + \beta_i}$ divise $|c|$. $\square$ (Autre preuve : c est un multiple commun de a et b , donc de $a \vee b = |ab|$.)

Contre-exemple sans l'hypothèse : $6 \mid 18$ et $9 \mid 18$, mais $54 \nmid 18$ (car $6 \wedge 9 = 3$). **Applications :** pour montrer que $72 \mid N$, on montre $8 \mid N$ et $9 \mid N$ ($8 \wedge 9 = 1$) : c'est le cas de $N = 6\,237\,504$ (section 5) ; de même $36 = 4 \times 9$, $99 = 9 \times 11$, $24 = 3 \times 8$ (section 3).

Fraction irréductible ; écriture $a = da'$, $b = db'$

Soit $d = a \wedge b$ (avec a, b non nuls). 1. $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$, et $a \vee b = d |a'b'|$. 2. La fraction $\frac{a}{b}$ est **irréductible** lorsque $a \wedge b = 1$; pour rendre $\frac{a}{b}$ irréductible, on divise a et b par d : $\frac{a}{b} = \frac{a'}{b'}$.

Démonstration de 1. $d = (da') \wedge (db') = d(a' \wedge b')$ (homogénéité), donc $a' \wedge b' = 1$; puis $a \vee b = \frac{|ab|}{d} = \frac{d^2 |a'b'|}{d} = d |a'b'|$. $\square$

Fil rouge : $2520 = 126 \times 20$ et $1386 = 126 \times 11$, avec $20 \wedge 11 = 1$: $\frac{1386}{2520} = \frac{11}{20}$ est la forme irréductible, et $2520 \vee 1386 = 126 \times 20 \times 11 = 27\,720$.

Les cigales périodiques. En Amérique du Nord, certaines cigales sortent de terre tous les 13 ans, d'autres tous les 17 ans : deux couvées sorties ensemble en 1803 ressortent ensemble tous les $13 \vee 17 = 13 \times 17 = 221$ ans, ce qui s'est produit en 2024 dans l'Illinois. Selon une hypothèse des biologistes, ces périodes **premières** les protègent des prédateurs à cycle court ($4 \vee 13 = 52$).

11

Équations dans $\mathbb{Z}$

Méthode : Comment résoudre une équation dans $\mathbb{Z}$

1. Factoriser : se ramener à $A \times B = n$ (entier connu) ; alors A et B sont des **diviseurs associés** de n : $(A, B) = (d, \frac{n}{d})$ avec $d \in D(n)$, ce qui laisse un nombre fini de cas. **2. Restes :** comparer les restes des deux membres modulo un entier bien choisi (2, 3, 4, 8...) ; s'ils sont incompatibles, il n'y a pas de solution ; sinon, on restreint les inconnues. **3. Encadrer :** une inégalité borne une inconnue, et il ne reste qu'un nombre fini de cas à tester. **4. Vérifier** chaque solution trouvée (on a raisonné par conditions nécessaires) et conclure par l'ensemble des solutions.

Exemple : factoriser : $xy = n$, puis $xy + x - 2y = 7$ dans $\mathbb{Z}^2$

Les solutions de $xy = n$ ($n \neq 0$) sont les couples $(d, \frac{n}{d})$, $d \in D(n)$: il y en a deux fois plus que de diviseurs positifs ($xy = 12$: 12 couples). Pour $xy + x - 2y = 7$, on fait apparaître un produit : $(x - 2)(y + 1) = xy + x - 2y - 2$, donc l'équation équivaut à $(x - 2)(y + 1) = 5$. Les cas $(x - 2, y + 1) \in \{(1, 5), (5, 1), (-1, -5), (-5, -1)\}$ donnent $S = \{(3, 4), (7, 0), (1, -6), (-3, -2)\}$ (contrôle : $(-3)(-2) - 3 + 4 = 7$).

Exemple : une différence de carrés : $x^2 - y^2 = 48$ dans $\mathbb{N}^2$

$(x - y)(x + y) = 48$ avec $0 \leq x - y \leq x + y$. De plus $x - y$ et $x + y$ ont la **même parité** (leur somme $2x$ est paire). Parmi $1 \times 48, 2 \times 24, 3 \times 16, 4 \times 12, 6 \times 8$, seuls $2 \times 24, 4 \times 12, 6 \times 8$ conviennent ; on résout $x - y = u, x + y = v$: $x = \frac{u+v}{2}, y = \frac{v-u}{2}$: $S = \{(13, 11), (8, 4), (7, 1)\}$.

Quels entiers sont des différences de deux carrés ? n impair : $n = (\frac{n+1}{2})^2 - (\frac{n-1}{2})^2$; $4 \mid n$: $n = (\frac{n}{4} + 1)^2 - (\frac{n}{4} - 1)^2$; $n \equiv 2 \pmod{4}$: **jamais**, car un carré est $\equiv 0$ ou $1 \pmod{4}$, donc $x^2 - y^2 \equiv 0, 1$ ou $3 \pmod{4}$.

Exemple : par les restes, puis par encadrement

1. L'équation $y^2 - 3x^2 = 2$ n'a **aucune** solution dans $\mathbb{Z}^2$: elle donnerait $y^2 \equiv 2 \pmod{3}$, alors qu'un carré est $\equiv 0$ ou $1 \pmod{3}$ (section 3).
2. $x^2 + xy + y^2 = 49$ dans $\mathbb{N}^2$. Par symétrie, cherchons d'abord les solutions avec $x \geq y$: alors $3y^2 \leq x^2 + xy + y^2 = 49$, donc $y \leq 4$. On teste : $y = 0$: $x^2 = 49, x = 7$; $y = 1$: $x^2 + x = 48$, impossible ($6 \times 7 = 42, 7 \times 8 = 56$) ; $y = 2$: $(x + 1)^2 = 46$, impossible ; $y = 3$: $x^2 + 3x - 40 = (x + 8)(x - 5) = 0, x = 5$; $y = 4$: $(x + 2)^2 = 37$, impossible. Avec les symétriques : $S = \{(7, 0), (5, 3), (3, 5), (0, 7)\}$.

Exemple : congruences $ax \equiv b [n]$: on teste les n restes

1. $5x \equiv 4 [7]$: on lit la ligne de 5 dans la table de la section 4 (ou le tableau ci-contre) : seul

$x \equiv 5$ convient ($25 \equiv 4$) : $x \equiv 5 [7]$, soit

$x = 5 + 7k, k \in \mathbb{Z}$.

2. $6x \equiv 3 [9]$: $x \equiv 2, 5$ ou $8 [9]$, c'est-à-dire

$x \equiv 2 [3]$. 3. $6x \equiv 4 [9]$: **aucune** solution ($6x$ n'est congru qu'à 0, 3 ou 6).

4. $x^2 + x + 5 \equiv 0 [7]$: $x \equiv 1$ ou $x \equiv 5 [7]$.

$x \equiv$	0	1	2	3	4	5	6	7	8
$5x [7]$	0	5	3	1	6	4	2		
$x^2 + x + 5 [7]$	5	0	4	3	4	0	5		
$6x [9]$	0	6	3	0	6	3	0	6	3

Exemple : un système : $a \wedge b = 18$ et $a \vee b = 1080$, avec $0 < a \leq b$

On écrit $a = 18a'$, $b = 18b'$ avec $a' \wedge b' = 1$ et $a' \leq b'$; alors $a \vee b = 18a'b'$, donc $a'b' = 60 = 2^2 \cdot 3 \cdot 5$. Les couples de diviseurs associés de 60 **premiers entre eux** sont (1, 60), (3, 20), (4, 15), (5, 12) (on écarte (2, 30) et (6, 10), de PGCD 2). Réciproquement, ces couples conviennent ($a \wedge b = 18(a' \wedge b') = 18$ et $a \vee b = 18a'b' = 1080$) : $(a, b) \in \{(18, 1080), (54, 360), (72, 270), (90, 216)\}$.

12**Pour aller plus loin**

1. **Numération en base $b \geq 2$.** Tout entier $N \geq 1$ s'écrit de façon unique $N = a_m b^m + \dots + a_1 b + a_0 = \overline{a_m \dots a_0}^{(b)}$, avec des chiffres $a_i \in \{0, \dots, b-1\}$, $a_m \neq 0$: ce sont les **restes des divisions successives par b** : $2026 = 8 \times 253 + 2$, $253 = 8 \times 31 + 5$, $31 = 8 \times 3 + 7$, $3 = 8 \times 0 + 3$, donc $2026 = \overline{3752}^{(8)}$; $\overline{10110}^{(2)} = 16 + 4 + 2 = 22$. Comme $b \equiv 1 [b-1]$, $N \equiv a_0 + \dots + a_m [b-1]$ (le critère par 9) : $3 + 7 + 5 + 2 = 17 \equiv 3 \equiv 2026 [7]$.

2. **Nombres parfaits.** n est **parfait** si $\sigma(n) = 2n$ (il est la somme de ses diviseurs autres que lui-même) : $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, 496 , 8128 . **Théorème (Euclide)** : si $q = 2^k - 1$ est premier, alors $n = 2^{k-1}q$ est parfait. En effet (section 7) : $\sigma(n) = (2^k - 1)(1 + q) = q \times 2^k = 2n$. Euler a montré que tous les nombres parfaits **pairs** sont de cette forme ; on ignore encore s'il existe un nombre parfait impair.

3. **L'exposant de p dans $n!$ (formule de Legendre).** Parmi $1, 2, \dots, n$, il y a $E\left(\frac{n}{p}\right)$ multiples de p (car $kd \leq n \iff k \leq \frac{n}{d}$). Chaque multiple de p apporte un facteur p , chaque multiple de p^2

un deuxième, etc. : $v_p(n!) = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \dots$ (somme finie). Un zéro final vient d'un facteur $10 = 2 \times 5$, et les facteurs 2 sont plus nombreux que les facteurs 5 : $125!$ se termine par $25 + 5 + 1 = \boxed{31}$ zéros.

4. **Les nombres de Mersenne** $M_n = 2^n - 1$. Si $n = ab$ avec $1 < a < n$, alors $2^a - 1$ divise $(2^a)^b - 1$ (car $x-1 \mid x^b-1$, section 14) et $1 < 2^a - 1 < 2^n - 1$: **si M_n est premier, alors n est premier**. La réciproque est fautive : $M_{23} = 8\,388\,607 = 47 \times 178\,481$. En octobre 2024, le plus grand nombre premier connu était $M_{136\,279\,841}$, qui a plus de 41 millions de chiffres.

5. En 2^e Bac SM, ce chapitre se prolonge par le **théorème de Bézout**, le **théorème de Gauss** et le **petit théorème de Fermat** : ils permettront de démontrer le lemme admis en section 6 et d'aller plus loin dans l'étude des restes des puissances.

13

Les pièges classiques

X Faux	✓ Vrai
« $a \mid bc$, donc $a \mid b$ ou $a \mid c$ »	vrai seulement si a est premier (lemme) : $6 \mid 4 \times 9$, mais $6 \nmid 4$ et $6 \nmid 9$
« $-23 = 5 \times (-4) - 3$: le reste de -23 par 5 est -3 »	un reste est positif ou nul : $-23 = 5 \times (-5) + 2$, le reste est 2
« $ab \equiv 0 [n]$, donc $a \equiv 0$ ou $b \equiv 0 [n]$ »	$4 \times 6 = 24 \equiv 0 [8]$; c'est vrai si n est premier (lemme)
« $4x \equiv 4y [6]$, donc $x \equiv y [6]$ » (on simplifie par 4)	on ne divise pas une congruence : $4 \times 1 \equiv 4 \times 4 [6]$, mais $1 \not\equiv 4 [6]$
« $a \equiv b [n]$, donc $c^a \equiv c^b [n]$ »	on ne réduit pas les exposants modulo n : $1 \equiv 6 [5]$, mais $2^1 = 2$ et $2^6 = 64 \equiv 4 [5]$
« 1 est premier »	1 n'a qu'un diviseur positif ; sinon la décomposition ne serait plus unique : $6 = 2 \times 3 = 1 \times 2 \times 3$
« 91 n'est divisible ni par 2, ni par 3, ni par 5 : il est premier »	il faut tester tous les premiers $p \leq \sqrt{91}$, donc aussi 7 : $91 = 7 \times 13$
« $n! + 1$ est premier », « $p_1 p_2 \dots p_k + 1$ est premier »	$4! + 1 = 25$; on sait seulement que ses facteurs premiers sont $> n$ (section 6)
« $a \mid c$ et $b \mid c$, donc $ab \mid c$ » ; « $a \vee b = ab$ »	il faut $a \wedge b = 1$: $6 \mid 18, 9 \mid 18$, mais $54 \nmid 18$; $6 \vee 9 = 18$
« PGCD : les plus grands exposants »	PGCD : facteurs communs, plus petits exposants ; PPCM : tous les facteurs, plus grands exposants
« $(-12) \wedge 18 = -6$ » ; « $D(6) = \{1, 2, 3, 6\}$ »	un PGCD est ≥ 1 : $(-12) \wedge 18 = 6$; dans $\mathbb{Z}$, $D(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$
« $72 = 2^3 \cdot 3^2$ a $3 \times 2 = 6$ diviseurs »	on compte aussi l'exposant 0 : $(3+1)(2+1) = 12$ diviseurs positifs
« $x^2 \equiv 1 [n]$, donc $x \equiv \pm 1 [n]$ »	$3^2 = 9 \equiv 1 [8]$ et $3 \not\equiv \pm 1 [8]$ (modulo 8, tout impair convient)

14

Les astuces des concours

★ Astuce de concours : le PGCD divise toute combinaison (OIM 1959)

Pour tout $n \in \mathbb{N}$, la fraction $\frac{21n+4}{14n+3}$ est irréductible : $d = (21n+4) \wedge (14n+3)$ divise $3(14n+3) - 2(21n+4) = 1$, donc $d = 1$. On a choisi 3 et 2 pour éliminer n : $3 \times 14 = 2 \times 21$.

★ Astuce de concours : travailler modulo un petit nombre bien choisi

$2^n + 1$ n'est jamais divisible par 7 : $2^3 = 8 \equiv 1 [7]$, donc 2^n est congru à 1, 2 ou 4 modulo 7, et $2^n + 1 \equiv 2, 3$ ou 5, jamais à 0. **Réflexe** : pour des carrés, travailler modulo 3, 4, 5 ou 8 ; pour des cubes, modulo 7 ou 9 ; pour des puissances de a , modulo un n où le cycle de a est court.

★ **Astuce de concours : repérer le cycle, même pour un exposant géant**

Un classique : $7 \mid 2222^{5555} + 5555^{2222}$. En effet $2222 \equiv 3$ et $5555 \equiv 4 \pmod{7}$; $3^6 \equiv 1$ et $5555 = 6 \times 925 + 5$, donc $3^{5555} \equiv 3^5 = 243 \equiv 5$; $4^3 \equiv 1$ et $2222 = 3 \times 740 + 2$, donc $4^{2222} \equiv 16 \equiv 2$; et $5 + 2 = 7 \equiv 0 \pmod{7}$.

Une tour : le chiffre des unités de 7^{7^7} . Les puissances de 7 ont un cycle de longueur 4 modulo 10 (7, 9, 3, 1) : il suffit de connaître l'exposant 7^7 modulo 4. Or $7 \equiv -1 \pmod{4}$, donc $7^7 \equiv -1 \equiv 3 \pmod{4}$, et $7^{7^7} \equiv 7^3 = 343$: le chiffre des unités est $\boxed{3}$.

★ **Astuce de concours : factoriser $a^n - b^n$ et $a^n + b^n$**

$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$, donc $a - b \mid a^n - b^n$; et pour n impair (remplacer b par $-b$), $a + b \mid a^n + b^n$.

1. $n^3 - 1 = (n - 1)(n^2 + n + 1)$ est premier ($n \in \mathbb{N}$) $\iff n = 2$: si $n \geq 3$, les deux facteurs sont ≥ 2 ; $n = 0, 1, 2$ donnent $-1, 0, 7$.

2. $2027 \mid 1^{2027} + 2^{2027} + \dots + 2026^{2027}$: on groupe les 2026 termes en 1013 paires $k^{2027} + (2027 - k)^{2027}$, chacune divisible par $k + (2027 - k) = 2027$, car l'exposant 2027 est impair.

★ **Astuce de concours : encadrer entre deux carrés consécutifs**

Pour quels $n \in \mathbb{N}$ le nombre $n^2 + 3n + 7$ est-il un carré ? Pour $n \geq 4$: $(n + 1)^2 = n^2 + 2n + 1 < n^2 + 3n + 7 < n^2 + 4n + 4 = (n + 2)^2$ (la seconde inégalité équivaut à $n > 3$) ; or il n'y a aucun carré strictement entre deux carrés consécutifs. On teste $n \in \{0, 1, 2, 3\}$: 7, 11, 17, 25 : seul $n = 3$ convient ($25 = 5^2$).

★ **Astuce de concours : carrés modulo 3, 4 et 8 (triangles rectangles)**

Si $a^2 + b^2 = c^2$ (entiers), alors $12 \mid ab$ (3, 4, 5 : 12 ; 5, 12, 13 : 60 ; 8, 15, 17 : 120). **Par 3 :** si $3 \nmid a$ et $3 \nmid b$, alors $a^2 + b^2 \equiv 1 + 1 = 2 \pmod{3}$, impossible pour un carré. **Par 4 :** a et b ne sont pas tous deux impairs (sinon $c^2 \equiv 2 \pmod{4}$). S'ils sont tous deux pairs, $4 \mid ab$. Sinon, disons a impair et $b = 2m$; alors c est impair et $b^2 = c^2 - a^2 \equiv 1 - 1 = 0 \pmod{8}$ (carrés impairs, section 3) : $8 \mid 4m^2$, donc m est pair et $4 \mid b$. **Enfin** $3 \mid ab$, $4 \mid ab$ et $3 \wedge 4 = 12 \mid ab$ (section 10).

15

L'essentiel du chapitre en une page

Divisibilité

$a \mid b \iff \exists k \in \mathbb{Z}, b = ka$; $a \mid b \iff |a| \mid |b|$; $a \mid 0$.

$a \mid b$ et $a \mid c \Rightarrow a \mid bu + cv$; $a \mid b, b \neq 0 \Rightarrow |a| \leq |b|$.

$a \mid b$ et $b \mid a \Rightarrow |a| = |b|$; $A(n) \mid B(n)$: éliminer n .

Division euclidienne ($b \neq 0$)

$a = bq + r$, $0 \leq r < |b|$, (q, r) unique ; $q = E\left(\frac{a}{b}\right)$ si $b > 0$.

$b \mid a \iff r = 0$; $n = 2k$ ou $2k + 1$; $3k$ ou $3k + 1$.

Restes

$n^2 \equiv 0, 1 \pmod{3}$; $n^2 \equiv 0, 1 \pmod{4}$; $n^2 \equiv 0, 1, 4 \pmod{8}$; n impair $\Rightarrow n^2 \equiv 1 \pmod{8}$.

$2 \mid n(n+1)$; $6 \mid n(n+1)(n+2)$.

Congruences

$a \equiv b \pmod{n} \iff n \mid a - b \iff$ même reste par n .

$a \equiv b, c \equiv d \Rightarrow a \pm c \equiv b \pm d, ac \equiv bd, a^k \equiv b^k \pmod{n}$.

On **ne divise pas** une congruence ; on ne réduit pas les exposants.

Grande puissance : $a^k \equiv 1$ (ou -1), $N = kq + s$, $a^N \equiv a^s$ (ou $(-1)^q a^s$).

Critères (S = somme des chiffres)

$N \equiv S \pmod{9}$ (et $\pmod{3}$) ; $N \equiv a_0 - a_1 + a_2 - \dots \pmod{11}$; 4 : deux derniers chiffres ; 8 : trois derniers ; 2, 5 : chiffre des unités.

Nombres premiers

Plus petit diviseur > 1 : premier ; n composé $\Rightarrow$ il a un diviseur premier $p \leq \sqrt{n}$.

Infinité : un facteur premier de $n! + 1$ est $> n$.

$p \geq 5$ premier $\Rightarrow p \equiv \pm 1 \pmod{6}$; $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.

Décomposition $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (unique)

Diviseurs : $p_1^{\beta_1} \dots p_k^{\beta_k}$, $0 \leq \beta_i \leq \alpha_i$; nombre $(\alpha_1 + 1) \dots (\alpha_k + 1)$.

$\sigma(n) = \prod \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$; carré $\iff$ exposants pairs $\iff$ nombre de diviseurs impair.

PGCD et PPCM

$a = bq + r \Rightarrow a \wedge b = b \wedge r$; Euclide : dernier reste non nul.

$D(a) \cap D(b) = D(a \wedge b)$; $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

$a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}$; $a \vee b = \prod p_i^{\max(\alpha_i, \beta_i)}$.

$(a \wedge b)(a \vee b) = |ab|$; $(ka) \wedge (kb) = |k|(a \wedge b)$.

Premiers entre eux ($a \wedge b = 1$)

$\iff$ aucun facteur premier commun

$\iff a \vee b = |ab|$.

$a \mid c, b \mid c, a \wedge b = 1 \Rightarrow ab \mid c$.

$d = a \wedge b : a = da', b = db', a' \wedge b' = 1$,

$a \vee b = d|a'b'|$.

Équations dans $\mathbb{Z}$

Factoriser ($A \times B = n$: diviseurs associés) ;

$x^2 - y^2 : x - y$ et $x + y$ de même parité ; restes

(modulo 3, 4, 8) ; encadrer, puis tester ;

$ax \equiv b \pmod{n}$: tester les n restes.

Système $a \wedge b = d, a \vee b = m : a'b' = \frac{m}{d}, a' \wedge b' = 1$.

À retenir pour les concours

$a - b \mid a^n - b^n$; $a + b \mid a^n + b^n$ (n impair).

$v_p(n!) = \sum_k E\left(\frac{n}{p^k}\right)$; $2^n - 1$ premier $\Rightarrow n$ premier.

Le PGCD divise toute combinaison ; aucun carré entre m^2 et $(m+1)^2$.

Bon courage ! La régularité bat le talent.

Maths Olympiad

Partie B • Le parcours

30 exercices sur 4 niveaux, du plus simple au niveau concours

Notations du cours : $a \mid b$ (a divise b), $a \nmid b$; $D(n)$ diviseurs de n dans $\mathbb{Z}$; $n\mathbb{Z}$ multiples de n ; $a \equiv b [n]$; $a \wedge b$ et $a \vee b$ PGCD et PPCM ; $E(x)$ partie entière ; $x13y$ nombre écrit en base dix avec les chiffres $x, 1, 3, y$; un carré parfait est le carré d'un entier.

16

Niveau 1 • Bases

Exercice 1 Diviseurs et multiples dans $\mathbb{Z}$ ★

corrigé p. 40

- Déterminer l'ensemble $D(-20)$ des diviseurs de -20 dans $\mathbb{Z}$. Combien a-t-il d'éléments ?
- Vrai ou faux ? Justifier. a) $-7 \mid 91$; b) $12 \mid -84$; c) $0 \mid 6$; d) $9 \mid 0$; e) $-5 \in 15\mathbb{Z}$; f) $45 \in 9\mathbb{Z} \cap 15\mathbb{Z}$.
- Soit $n \in \mathbb{Z}$ et d un diviseur commun de $4n + 7$ et de $3n + 5$. Montrer que $d \mid 1$; que vaut d ?
- Déterminer les entiers $n \in \mathbb{Z}$ tels que : a) $n + 4 \mid 3n + 5$; b) $2n + 1 \mid n + 7$.

Exercice 2 La division euclidienne dans $\mathbb{Z}$ ★

corrigé p. 40

- Écrire la division euclidienne ($a = bq + r$, $0 \leq r < |b|$) : a) de 389 par 17 ; b) de -389 par 17 ; c) de 389 par -17 ; d) de -389 par -17 . Dans b), placer -389 entre deux multiples consécutifs de 17 (droite graduée) et vérifier que $q = E\left(\frac{-389}{17}\right)$.
- Déterminer les entiers naturels n tels que le quotient de la division euclidienne de 100 par n soit 7 ; préciser le reste.
- Le reste de la division euclidienne de l'entier a par 6 est 4. Quels sont les restes des divisions par 6 de $-a$, de $2a$ et de a^2 ? Et le reste de la division de a par 3 ?

Exercice 3 Parité et disjonction des cas ★

corrigé p. 41

- Montrer que, pour tout $n \in \mathbb{Z}$: a) $(n + 2)(n + 5)$ est pair ; b) $n^2 + n + 1$ est impair.
- À l'aide d'un tableau des restes de n dans la division par 3, montrer que $3 \mid n(n + 4)(2n + 1)$ pour tout $n \in \mathbb{Z}$.
- a) Quels sont les restes possibles de $n(n + 1)$ dans la division par 10 ($n \in \mathbb{N}$) ? b) En déduire que le chiffre des unités de $n^2 + n + 1$ est 1, 3 ou 7.

Exercice 4 Premières congruences ★

corrigé p. 41

- Vrai ou faux ? a) $47 \equiv 5 [7]$; b) $-13 \equiv 8 [7]$; c) $100 \equiv -1 [101]$; d) $2026 \equiv 2 [5]$; e) $38 \equiv -2 [9]$.
- On sait que $a \equiv 3 [7]$ et $b \equiv 5 [7]$. Déterminer les restes par 7 de $a + b$, ab , $a - b$, $a^2 + b^2$, a^3 et $2a - 3b + 1$. 3. Vérifier que $3^3 \equiv 1 [13]$; en déduire les restes par 13 de 3^{1000} et de 29^{1000} .
- En testant les restes possibles, résoudre dans $\mathbb{Z}$: a) $x + 4 \equiv 1 [6]$; b) $3x \equiv 2 [7]$; c) $4x \equiv 2 [6]$; d) $x^2 \equiv 4 [5]$; e) $2x \equiv 1 [4]$.

Exercice 5 Reconnaître un nombre premier ★

corrigé p. 41

1. Parmi 253, 257, 299, 307, 361, 377 et 409, lesquels sont premiers ? (Critère : aucun diviseur premier $p \leq \sqrt{n}$.)
2. Soit p un nombre premier impair. a) Vérifier que $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$. b) Montrer que c'est la seule écriture $p = x^2 - y^2$ avec $x, y \in \mathbb{N}$. c) Écrire 409 comme différence de deux carrés.

Exercice 6 Décomposition en facteurs premiers ★

corrigé p. 42

Soit $A = 1176$ et $B = 1260$.

1. Décomposer A et B en produit de facteurs premiers. 2. Nombre de diviseurs de A , de B , dans $\mathbb{N}$ et dans $\mathbb{Z}$?
3. Calculer $A \wedge B$ et $A \vee B$ à l'aide des décompositions ; vérifier que $(A \wedge B)(A \vee B) = AB$.
4. Déterminer le plus petit entier $k \in \mathbb{N}^*$ tel que kA soit un carré parfait ; même question pour B .

Exercice 7 L'algorithme d'Euclide ★

corrigé p. 42

1. Calculer $1517 \wedge 1189$ par l'algorithme d'Euclide (présenter les divisions successives dans un tableau). En déduire $1517 \vee 1189$ et la forme irréductible de la fraction $\frac{1189}{1517}$.
2. En déduire, sans nouvel algorithme, $3034 \wedge 2378$ et $(-4551) \wedge 3567$. 3. Soit $n \in \mathbb{Z}$: montrer que $n \wedge (3n + 1) = 1$ et que $(2n + 1) \wedge (2n + 3) = 1$.

Exercice 8 Critères de divisibilité ★

corrigé p. 42

1. Sans poser de division, dire si 7 425 et 123 456 sont divisibles par 2, 3, 4, 5, 8, 9 et 11.
2. Déterminer les chiffres x et y tels que $\overline{3x7y}$ soit divisible par 45. 3. Déterminer les chiffres $x \neq 0$ et y tels que $x13y$ soit divisible par 99.

17

Niveau 2 · Bac**Exercice 9** Type devoir surveillé (1) : division euclidienne et restes ★★

corrigé p. 43

Soit $n \in \mathbb{Z}$.

1. a) Vérifier que $n^2 + 4n + 9 = (n + 3)(n + 1) + 6$. b) Pour $n \in \mathbb{N}$, $n \geq 4$, en déduire le quotient et le reste de la division euclidienne de $n^2 + 4n + 9$ par $n + 3$. Est-ce encore le cas pour $n = 1$? c) Déterminer les entiers $n \in \mathbb{Z}$ tels que $n + 3 \mid n^2 + 4n + 9$.
2. a) Dresser le tableau des restes de $n^2 + n + 7$ dans la division par 9, selon le reste de n par 9. b) En déduire que $9 \mid n^2 + n + 7$ si et seulement si n a pour reste 1 dans la division par 3. c) On écrit alors $n = 3k + 1$: montrer que $n^2 + n + 7 = 9(k^2 + k + 1)$ et, selon le reste de k par 3, que $9 \nmid k^2 + k + 1$. d) Conclure : $81 \nmid n^2 + n + 7$.

Exercice 10 Type devoir surveillé (2) : congruences et puissances ★★

corrigé p. 43

1. a) Vérifier que $3^5 \equiv 1 [11]$; en déduire le reste de 3^n par 11 selon le reste de n par 5 ($n \in \mathbb{N}$). b) Déterminer les restes par 11 de 3^{999} , de 47^{2027} et de 5^{100} (vérifier que $5 \equiv 3^3 [11]$). c) Déterminer les $n \in \mathbb{N}$ tels que $11 \mid 3^n + 2$. Montrer que $11 \nmid 3^n + 1$ pour tout $n \in \mathbb{N}$.
2. Vérifier que $256 \equiv 3 [11]$; en déduire que $11 \mid 3^{n+3} - 4^{4n+2}$ pour tout $n \in \mathbb{N}$.
3. Déterminer le chiffre des unités de 3^{999} . Montrer que $3^{999} + 7^{999}$ est divisible par 10.

Exercice 11 Type devoir surveillé (3) : PGCD et PPCM ★★

corrigé p. 43

1. a) Calculer $4199 \wedge 2431$ par l'algorithme d'Euclide ; en déduire $4199 \vee 2431$. b) Simplifier $\frac{2431}{4199}$.
2. Soit $n \in \mathbb{N}$, $a = n + 4$ et $b = n^2 + 5n + 15$. a) Montrer que $a \wedge b = a \wedge 11$. b) En déduire les valeurs possibles de $a \wedge b$, puis les entiers n pour lesquels la fraction $\frac{b}{a}$ est irréductible. c) Cas $n = 18$?
3. Déterminer les couples $(a, b) \in \mathbb{N}^2$ tels que $a \leq b$, $a \wedge b = 21$ et $a \vee b = 2310$. Lequel vérifie $a + b = 441$?

Exercice 12 Type devoir surveillé (4) : nombres premiers et décomposition ★★

corrigé p. 44

1. a) Combien de diviseurs positifs a l'entier $N = 2^a 3^b$ ($a, b \in \mathbb{N}$) ? b) Déterminer les entiers $N = 2^a 3^b$ divisibles par 36 et ayant exactement 15 diviseurs positifs. c) Vérifier que ce sont des carrés parfaits : était-ce prévisible ?
2. a) Vérifier que $n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1)$. b) Pour quels $n \in \mathbb{N}$ l'entier $n^4 + n^2 + 1$ est-il premier ?
3. Soit p un nombre premier. a) Montrer que si $p \neq 3$, alors $3 \mid 8p^2 + 1$. b) Déterminer les nombres premiers p tels que $8p^2 + 1$ soit premier.

Exercice 13 Critères de divisibilité par 7, 11 et 13 ★★

corrigé p. 44

1. Vérifier que $1001 = 7 \times 11 \times 13$. En déduire que $1000 \equiv -1$ modulo 7, modulo 11 et modulo 13.
2. On écrit $N \in \mathbb{N}$ par tranches de trois chiffres : $N = t_0 + 1000t_1 + \dots + 1000^k t_k$ ($0 \leq t_i \leq 999$). Montrer que $N \equiv t_0 - t_1 + t_2 - \dots + (-1)^k t_k \pmod{1001}$; en déduire des critères de divisibilité par 7, 11, 13.
3. Applications : a) restes de 2 718 281 828 dans les divisions par 7, 11 et 13 ; b) montrer que tout nombre $\overline{abcabc}$ est divisible par 7, 11 et 13.
4. Soit $N = 10a + u$, avec $a \in \mathbb{N}$ et u le chiffre des unités de N . Montrer que $7 \mid N \iff 7 \mid a - 2u$; cas $N = 3157$?

Exercice 14 Équations : factoriser, comparer les restes ★★

corrigé p. 44

1. Résoudre dans $\mathbb{Z}^2$ l'équation $xy - 2x - 3y = 0$ (développer $(x - 3)(y - 2)$).
2. Résoudre dans $\mathbb{N}^2$ l'équation $x^2 - y^2 = 45$ (parités de $x - y$ et $x + y$). Combien a-t-elle de solutions dans $\mathbb{Z}^2$?
3. a) Quels sont les restes possibles d'un carré dans la division par 5 ? b) Montrer que l'équation $x^2 - 5y^2 = 2027$ n'a pas de solution dans $\mathbb{Z}^2$.

Exercice 15 Congruences du premier et du second degré ★★

corrigé p. 45

1. En testant les restes, résoudre dans $\mathbb{Z}$: a) $5x \equiv 3 \pmod{8}$; b) $6x \equiv 9 \pmod{15}$; c) $4x \equiv 7 \pmod{10}$.
2. Résoudre dans $\mathbb{Z}$: a) $x^2 + x + 1 \equiv 0 \pmod{7}$; b) $x^2 \equiv x \pmod{12}$. Que remarque-t-on dans b) ?
3. a) Résoudre le système $x \equiv 2 \pmod{3}$ et $x \equiv 3 \pmod{5}$ (écrire $x = 3k + 2$). b) Un panier contient entre 100 et 120 œufs. Rangés par 3, il en reste 2 ; rangés par 5, il en reste 3. Combien y en a-t-il ?

Exercice 16 Nombres premiers entre eux ★★

corrigé p. 45

1. Soit $n \in \mathbb{Z}$. a) Montrer que $3 \mid n^4 - n^2$ et que $4 \mid n^4 - n^2$. b) En déduire que $12 \mid n^4 - n^2$. A-t-on $24 \mid n^4 - n^2$ pour tout n ?
2. Montrer que, pour tout $n \in \mathbb{N}$, la fraction $\frac{2n+3}{5n+7}$ est irréductible. 3. Déterminer les couples $(a, b) \in \mathbb{N}^2$ tels que $a + b = 120$ et $a \wedge b = 15$ (écrire $a = 15a'$ et $b = 15b'$).

18

Niveau 3 · Approfondissement

Exercice 17 La factorisation de $a^n - b^n$ et le PGCD ★★★

corrigé p. 45

1. a) Rappeler pourquoi $a - b \mid a^n - b^n$ ($a, b \in \mathbb{Z}, n \in \mathbb{N}^*$). b) En déduire que 7 et 31 divisent $2^{15} - 1$, puis décomposer $2^{15} - 1$ en facteurs premiers.
2. Soit $a \geq b \geq 1$ deux entiers. a) Vérifier que $2^a - 1 = 2^{a-b}(2^b - 1) + (2^{a-b} - 1)$. b) En déduire que $(2^a - 1) \wedge (2^b - 1) = (2^{a-b} - 1) \wedge (2^b - 1)$. c) Par récurrence forte sur $a + b$, montrer que $(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$ pour tous $a, b \in \mathbb{N}^*$.
3. Calculer $(2^{84} - 1) \wedge (2^{60} - 1)$; montrer que $2^{2026} - 1$ et $2^{2025} - 1$ sont premiers entre eux.

Exercice 18 Cubes modulo 9 ★★★

corrigé p. 46

1. Montrer que, pour tout $x \in \mathbb{Z}$, $x^3 \equiv 0, 1$ ou -1 [9] (écrire $x = 3k, 3k + 1$ ou $3k - 1$).
2. En déduire qu'un entier congru à 4 ou à 5 modulo 9 n'est pas la somme de trois cubes d'entiers. L'entier 2030 est-il la somme de trois cubes ? 3. Montrer que si $9 \mid x^3 + y^3 + z^3$, alors $3 \mid xyz$.
4. Déterminer de deux façons le reste par 9 de $S = 1^3 + 2^3 + \dots + 100^3$: avec 1., puis avec la formule $1^3 + 2^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Exercice 19 Encadrer pour conclure ★★★

corrigé p. 46

1. On veut résoudre dans $\mathbb{Z}^2$ l'équation $x^3 - y^3 = 91$. a) Montrer que $x > y$ et que $d = x - y$ est un diviseur positif de 91. b) Vérifier que $4(x^2 + xy + y^2) = 3(x + y)^2 + d^2$; en déduire que $d^3 \leq 364$, puis résoudre l'équation.
2. Résoudre dans $(\mathbb{N}^*)^3$ l'équation $xyz = 2(x + y + z)$ (supposer d'abord $x \leq y \leq z$ et montrer que $xy \leq 6$).

Exercice 20 La somme des diviseurs ★★★

corrigé p. 46

Pour $n \in \mathbb{N}^*$, $\sigma(n)$ est la somme des diviseurs positifs de n . On rappelle (cours) que, si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, alors $\sigma(n) = \sigma(p_1^{\alpha_1}) \dots \sigma(p_k^{\alpha_k})$.

1. a) Calculer $\sigma(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}$. b) Calculer $\sigma(2^a 3^b)$. c) Déterminer les entiers $n = 2^a 3^b$ ($a, b \in \mathbb{N}$) tels que $\sigma(n) = 1240$.
2. a) Soit p un nombre premier impair. Montrer que $\sigma(p^\alpha)$ est impair si et seulement si α est pair. b) En déduire que $\sigma(n)$ est impair si et seulement si n est un carré parfait ou le double d'un carré parfait. c) Vérifier avec $n = 18$ et $n = 12$.

Exercice 21 PGCD et PPCM : des équations ★★★

corrigé p. 47

Pour $a, b \in \mathbb{N}^*$, on note $d = a \wedge b$ et $m = a \vee b$.

1. Déterminer les couples (a, b) tels que $d = 24$ et $a^2 + b^2 = 7488$. 2. Montrer que si $d + m = a + b$, alors $a \mid b$ ou $b \mid a$ (calculer $(a - d)(b - d)$ à l'aide de $dm = ab$).
3. Montrer que l'égalité $m = a + b$ est impossible. 4. Déterminer les couples (a, b) tels que $m = a + b + 3d$.

Exercice 22 Produits d'entiers consécutifs ★★★

corrigé p. 47

1. Montrer que, pour $n \in \mathbb{N}^*$, $n(n + 1)$ n'est pas un carré parfait (encadrer entre deux carrés).

2. a) Montrer que $n(n+1)(n+2)(n+3)+1=(n^2+3n+1)^2$. b) En déduire que le produit de quatre entiers naturels non nuls consécutifs n'est jamais un carré parfait. c) Calculer la racine carrée de $2023 \times 2024 \times 2025 \times 2026 + 1$.
3. a) Soit $a, b \in \mathbb{N}^*$ premiers entre eux tels que ab soit un carré parfait. À l'aide des décompositions, montrer que a et b sont des carrés parfaits. b) Montrer que $(n+1) \wedge n(n+2) = 1$, puis que le produit de trois entiers naturels non nuls consécutifs n'est jamais un carré parfait.

Exercice 23 Équations exponentielles ★★★

corrigé p. 47

Résoudre dans $\mathbb{N}^2$: a) $2^x - 1 = y^2$ (raisonner modulo 4) ; b) $2^x + 3 = y^2$; c) $2^x + 1 = y^2$ (factoriser $y^2 - 1$) ; d) $3^x + 1 = y^2$; e) $2^x + 1 = y^3$ (factoriser $y^3 - 1$).

19

Niveau 4 · Concours**Exercice 24 $n^5 - n$: restes et chiffres ★★★**

corrigé p. 47

1. Soit $n \in \mathbb{Z}$. a) Vérifier que $n^5 - n = (n-1)n(n+1)(n^2+1)$. b) En raisonnant sur les restes de n par 5, montrer que $5 \mid n^5 - n$; en déduire que $30 \mid n^5 - n$. c) Montrer que, si n est impair, alors $240 \mid n^5 - n$.
2. En déduire que n et n^5 ont le même chiffre des unités, puis que, pour tous $a, b, c \in \mathbb{Z}$: $30 \mid a+b+c \iff 30 \mid a^5+b^5+c^5$.
3. Déterminer le reste de la division euclidienne de $S = 1^5 + 2^5 + \dots + 2026^5$ par 30, puis le chiffre des unités de S . 4. Montrer que $30 \mid a^5b - ab^5$ pour tous $a, b \in \mathbb{Z}$.

Exercice 25 Sommes de carrés : restes et descente infinie ★★★

corrigé p. 48

1. Rappeler les restes possibles d'un carré modulo 8. En déduire qu'aucun entier de la forme $8k+7$ n'est la somme de trois carrés d'entiers ; exemple : 2023.
2. a) Montrer que si $x^2 + y^2 + z^2 \equiv 0 \pmod{4}$, alors x, y et z sont pairs. b) En déduire, par récurrence sur a , qu'aucun entier $4^a(8b+7)$ ($a, b \in \mathbb{N}$) n'est la somme de trois carrés. Exemples : 60 et 112.
3. Pour $k \in \mathbb{N}^*$, on note (E_k) l'équation $x^2 + y^2 + z^2 = 2^kxyz$, d'inconnue $(x, y, z) \in \mathbb{Z}^3$. a) Soit (x, y, z) une solution de (E_k) . Montrer que x, y, z sont pairs et que $(\frac{x}{2}, \frac{y}{2}, \frac{z}{2})$ est solution de (E_{k+1}) . b) En déduire que $(0, 0, 0)$ est la seule solution dans $\mathbb{Z}^3$ de $x^2 + y^2 + z^2 = 2xyz$.

Exercice 26 Divisibilité entre expressions polynomiales ★★★

corrigé p. 48

Soit $n \in \mathbb{Z}$ et $D = n^2 + n + 1$.

1. Montrer que $D \geq 1$ et que $n^3 \equiv 1 \pmod{D}$.
2. Soit $k \in \mathbb{N}$. Montrer que $D \mid n^{2k} + n^k + 1$ si $3 \nmid k$; et, si $3 \mid k$, que $D \mid n^{2k} + n^k + 1 \iff n \in \{-2, -1, 0, 1\}$.
3. Applications : a) montrer que $n^2 + n + 1 \mid n^{2026} + n^{1013} + 1$ pour tout $n \in \mathbb{Z}$; b) montrer que $4^k + 2^k + 1$ est composé pour tout entier $k \geq 2$ non multiple de 3.
4. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n^2 + n + 1 \mid n^4 + 3n + 5$.

Exercice 27 L'exposant de 2 dans $n!$ ★★★

corrigé p. 49

Pour $m \in \mathbb{N}^*$, $v(m)$ est l'exposant de 2 dans la décomposition de m . Soit $n \in \mathbb{N}^*$, écrit en base 2 : $n = a_r 2^r + \dots + a_1 2 + a_0$ ($a_i \in \{0, 1\}$, $a_r = 1$) ; $s(n) = a_0 + \dots + a_r$ est son nombre de chiffres 1.

1. Rappeler la formule de Legendre : $v(n!) = E\left(\frac{n}{2}\right) + E\left(\frac{n}{4}\right) + \dots + E\left(\frac{n}{2^r}\right)$. Calculer $v(2026!)$.

2. a) Montrer que, pour $1 \leq k \leq r$, $E\left(\frac{n}{2^k}\right) = a_r 2^{r-k} + \dots + a_{k+1} 2 + a_k$. b) En déduire que $v(n!) = n - s(n)$.
3. Applications : a) retrouver $v(2026!)$ en écrivant 2026 en base 2 ; b) montrer que 2^n ne divise jamais $n!$; c) déterminer les entiers $n \geq 1$ tels que $2^{n-1} \mid n!$.

Exercice 28 Fractions égyptiennes ★★★★★

corrigé p. 49

Soit $n \in \mathbb{N}^*$ et $(E) : \frac{1}{x} + \frac{1}{y} = \frac{1}{n}$, d'inconnue $(x, y) \in (\mathbb{Z}^*)^2$; $d(m)$ est le nombre de diviseurs positifs de $m \in \mathbb{N}^*$.

- Montrer que $(E) \iff (x - n)(y - n) = n^2$.
- a) Montrer que si $(x, y) \in (\mathbb{N}^*)^2$ est solution, alors $x > n$ et $y > n$. b) En déduire que (E) a exactement $d(n^2)$ solutions dans $(\mathbb{N}^*)^2$.
- Montrer que (E) a exactement $2d(n^2) - 1$ solutions dans $(\mathbb{Z}^*)^2$.
- Applications : a) résoudre (E) dans $(\mathbb{N}^*)^2$ pour $n = 10$ (avec $x \leq y$) ; b) nombre de solutions dans $(\mathbb{N}^*)^2$ et dans $(\mathbb{Z}^*)^2$ pour $n = 60$, puis pour $n = 2026$.

Exercice 29 La somme harmonique n'est jamais entière ★★★★★

corrigé p. 49

Pour $n \geq 2$, on pose $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$.

- Soit $k \in \mathbb{N}^*$ tel que $2^k \leq n < 2^{k+1}$. Montrer que 2^k est le seul multiple de 2^k dans $\{1, 2, \dots, n\}$.
- Soit M le produit des entiers impairs de $\{1, 2, \dots, n\}$ et $P = 2^{k-1}M$. Montrer que $\frac{P}{j}$ est un entier pour tout $j \in \{1, \dots, n\}$ différent de 2^k , mais que $\frac{P}{2^k}$ n'est pas un entier.
- En déduire que H_n n'est pas un entier. 4. Montrer de même que $1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n+1}$ ($n \geq 1$) n'est pas entier.

Exercice 30 Le défi de la couverture : les nombres de Fermat ★★★★★

corrigé p. 50

Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (nombres de Fermat).

- Calculer $F_0, \dots, F_4$ et montrer que $F_{n+1} - 2 = F_n (F_n - 2)$ pour tout $n \in \mathbb{N}$.
- Montrer par récurrence que, pour tout $n \in \mathbb{N}^*$, $F_0 F_1 \dots F_{n-1} = F_n - 2$.
- a) En déduire que deux nombres de Fermat distincts sont premiers entre eux. b) En déduire une nouvelle preuve de l'infinité des nombres premiers.
- Euler (1732) : $641 \mid F_5$. a) Vérifier que $641 = 5 \times 2^7 + 1 = 5^4 + 2^4$. b) Montrer que $5 \times 2^7 \equiv -1 \pmod{641}$, puis que $5^4 \times 2^{28} \equiv 1 \pmod{641}$. c) Avec $5^4 \equiv -2^4 \pmod{641}$, en déduire que $2^{32} \equiv -1 \pmod{641}$, donc $641 \mid F_5$.
- a) Montrer que si $2^m + 1$ ($m \in \mathbb{N}^*$) est premier, alors m est une puissance de 2 (si $m = qk$, $k \geq 3$ impair, utiliser $a + 1 \mid a^k + 1$). b) Montrer que le chiffre des unités de F_n est 7 si $n \geq 2$.

Partie C • La banque

36 exercices supplémentaires classés par thème, du niveau Bases au niveau Concours

20

Divisibilité et division euclidienne

Une combinaison qui élimine n ne donne qu'une condition **nécessaire** : on teste ensuite les candidats. Dans $a = bq + r : 0 \leq r < |b|$.

Exercice 31 Diviseurs et divisibilité ★

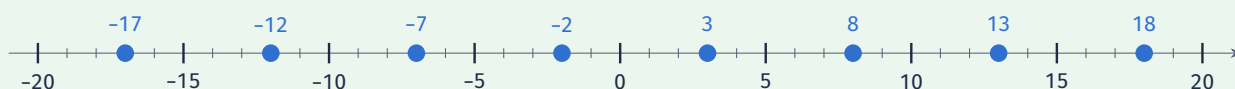
corrigé p. 50

- Déterminer l'ensemble $D(-48)$ et son nombre d'éléments, puis les entiers relatifs x tels que $x^2 - 1$ divise 48.
- Vrai ou faux ($a, b, c \in \mathbb{Z}$) ? Justifier. a) Si $a \mid b$, alors $a^2 \mid b^2$. b) Si $a \mid b^2$, alors $a \mid b$.
c) Si $a \mid b + c$ et $a \mid b$, alors $a \mid c$. d) Si $a \mid b + c$, alors $a \mid b$ ou $a \mid c$. e) Si $a \mid b$ et $a \mid c$, alors $a^2 \mid bc$.
- Montrer que, pour tout $n \in \mathbb{Z}$, $n(n + 1)$ est pair, puis que 8 divise $n(n + 1)(n^2 + n + 2)$ (poser $n(n + 1) = 2k$).

Exercice 32 Division euclidienne dans $\mathbb{Z}$ ★

corrigé p. 51

- On a marqué les entiers de $[-20, 20]$ dont le reste dans la division euclidienne par 5 est 3 :



- a) Écrire la division euclidienne par 5 de -17, de -2 et de 18. b) Décrire l'ensemble des entiers relatifs de reste 3 dans la division par 5. Combien y en a-t-il dans $[-100, 100]$?
- Déterminer les entiers relatifs a dont le quotient dans la division par 6 est égal au reste, puis ceux dont le quotient est l'opposé du reste.
- Soit $n \in \mathbb{N}$. Effectuer la division euclidienne de $-n^2$ par $n + 1$, puis, si $n \geq 1$, celle de $-n^2 - 1$ par n . En déduire, sans poser de division, celles de -2025 par 46 et de -2026 par 45.

Exercice 33 Quand $a(n)$ divise $b(n)$ ★★

corrigé p. 51

Dans chaque cas, déterminer l'ensemble des entiers relatifs n qui conviennent.

- a) $2n - 1 \mid 3n + 4$; b) $3n + 3 \mid 2n + 5$ (tous les candidats conviennent-ils ?) ; c) $2n + 1 \mid n^2 + 4$ (calculer $4(n^2 + 4) - (2n + 1)(2n - 1)$).
- $n^2 + 3 \mid n^2 + 2n + 9$. a) Montrer que la condition équivaut à $n^2 + 3 \mid 2(n + 3)$. b) Pour $n \neq -3$, en déduire que $n^2 + 3 \leq 2|n + 3|$, puis que $-1 \leq n \leq 3$. c) Conclure (sans oublier $n = -3$).

Exercice 34 Sommes de carrés consécutifs ★★

corrigé p. 52

1. Dresser le tableau des restes de n^2 dans la division par 5, puis par 4, selon le reste de n .
2. Soit $n \in \mathbb{Z}$. Montrer que la somme des carrés des quatre entiers $n - 1, \dots, n + 2$ vaut $4n^2 + 4n + 6$, celle des six entiers $n - 2, \dots, n + 3$ vaut $6n^2 + 6n + 19$, et que ce ne sont jamais des carrés parfaits.
3. a) Montrer que la somme S_5 des carrés de $n - 2, \dots, n + 2$ vaut $5(n^2 + 2)$. b) Montrer que $5 \nmid n^2 + 2$, et que $5 \mid m^2 \Rightarrow 25 \mid m^2$. c) En déduire que S_5 n'est jamais un carré.
4. Montrer que la somme des carrés de $n - 5, \dots, n + 5$ vaut $11(n^2 + 10)$, puis que $18^2 + 19^2 + \dots + 28^2$ est un carré parfait.

Exercice 35 Deux entiers qui se divisent ★★★

corrigé p. 52

On cherche les couples (a, b) d'entiers naturels **non nuls** ; si $d \mid m$ et $m \neq 0$, alors $|d| \leq |m|$.

1. Montrer que, si $ab \mid a + b$, alors $(a - 1)(b - 1) \leq 1$. Déterminer les couples tels que $ab \mid a + b$.
2. On suppose $a \mid b + 1$, $b \mid a + 1$ et $a \leq b$. a) Écrire $a + 1 = kb$ et montrer que $b = a + 1$ ou $a = b = 1$. b) Déterminer tous les couples (sans supposer $a \leq b$) tels que $a \mid b + 1$ et $b \mid a + 1$.
3. Déterminer de même tous les couples (a, b) tels que $a \mid b + 2$ et $b \mid a + 2$.

Exercice 36 Quand $1 + 2 + \dots + n$ divise $n!$ ★★★

corrigé p. 53

Pour $n \in \mathbb{N}^*$, on note $T_n = 1 + 2 + \dots + n = \frac{n(n+1)}{2}$ et $n! = 1 \times 2 \times \dots \times n$ (avec $0! = 1$).

1. Pour $1 \leq n \leq 6$, calculer T_n et $n!$, et dire si $T_n \mid n!$.
2. Montrer que $T_n \mid n!$ si et seulement si $n + 1 \mid 2(n - 1)!$.
3. Si $n + 1 = p$ est un premier impair, montrer que $p \nmid 2(n - 1)!$ (lemme : un premier qui divise un produit divise l'un des facteurs).
4. On suppose $n \geq 4$ et $n + 1 = ab$ non premier, avec $2 \leq a \leq b$. a) Si $a < b$, montrer que $b \leq n - 1$, puis que $ab \mid (n - 1)!$. b) Si $a = b$, montrer que $a \geq 3$ et que a et $2a$ sont deux facteurs distincts de $(n - 1)!$; en déduire que $a^2 \mid (n - 1)!$.
5. Conclure : pour quels entiers $n \geq 1$ a-t-on $T_n \mid n!$? Combien d'entiers $n \leq 100$ conviennent ?

21

Congruences

On ne réduit jamais un exposant modulo n : on cherche une puissance congrue à 1, qui crée un **cycle**, puis on dresse un tableau de restes.

Exercice 37 La preuve par 9 ★

corrigé p. 53

On note $S(N)$ la somme des chiffres de l'entier naturel N ; on rappelle (cours) que $N \equiv S(N) [9]$.

1. Montrer que, si $a \times b = c$, alors $S(a) \times S(b) \equiv S(c) [9]$ (principe de la *preuve par 9* : si cette congruence est fautive, le calcul est faux).
2. Faire la preuve par 9 de : a) $4567 \times 891 = 4\,069\,197$; b) $3109 \times 487 = 1\,504\,083$; c) $2347 \times 658 = 1\,544\,236$. Lesquels sont certainement faux ? Seul a) est juste : pourquoi l'erreur de c) n'est-elle pas détectée ?

3. On rappelle que $\overline{a_k \dots a_1 a_0} \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k$ [11]. Faire la *preuve par 11* de c), puis vérifier que le produit exact 1 544 326 passe les deux preuves.

Exercice 38 Puissances de 4 et de 7 modulo 9 ★

corrigé p. 54

1. Dresser le tableau des restes de 4^n et de 7^n modulo 9 pour $0 \leq n \leq 6$. Montrer que $4^{n+3} \equiv 4^n$ et $7^{n+3} \equiv 7^n$ [9].
2. Déterminer le reste de la division par 9 de 4^{2026} , de 7^{2027} et de $4^{2026} + 7^{2027}$.
3. Montrer que, pour tout $n \in \mathbb{N}$, 9 divise $4^n + 7^n - 2$.
4. Déterminer les entiers naturels n tels que $9 \mid 4^n + 5$, puis ceux tels que $9 \mid 7^n + 2 \times 4^n$.

Exercice 39 Palindromes et nombres retournés ★★

corrigé p. 54

On note $\overline{abc} = 100a + 10b + c$ ($a \neq 0$) ; un *palindrome* se lit de la même façon dans les deux sens.

1. Soit $N = \overline{abc}$ ($a \neq 0, c \neq 0$) et son retourné $N' = \overline{cba}$. Montrer que $N - N' = 99(a - c)$; en déduire que $9 \mid N - N'$ et $11 \mid N - N'$.
2. *Le tour du 1089*. Si $a \geq c + 2$, on calcule $D = N - N'$, puis $D + D'$ où D' est le retourné de D ($742 - 247 = 495$, $495 + 594 = 1089$). Avec $k = a - c$, montrer que $2 \leq k \leq 8$ et $D = 100(k - 1) + 90 + (10 - k)$; en déduire que l'on trouve toujours 1089.
3. Montrer que $\overline{aba} \equiv 2a - b$ [11]. Déterminer les palindromes à trois chiffres divisibles par 11.
4. Montrer que tout palindrome à quatre chiffres est divisible par 11 ; déterminer ceux qui sont divisibles par 99.

Exercice 40 Les deux derniers chiffres ★★

corrigé p. 54

Les deux derniers chiffres d'un entier naturel sont donnés par son reste modulo 100.

1. Vérifier que $76^2 \equiv 76$ [100], puis montrer par récurrence que $76^k \equiv 76$ [100] pour tout $k \in \mathbb{N}^*$.
2. Calculer 2^{10} , en déduire que $2^{20} \equiv 76$ [100], puis les deux derniers chiffres de 2^{2026} .
3. a) Montrer que $100 \mid 75 \times 2^n$ pour $n \geq 2$; en déduire que $2^{n+20} \equiv 2^n$ [100] pour tout $n \geq 2$. b) Dresser le tableau des restes de 2^n modulo 100 pour $2 \leq n \leq 21$; montrer que ce sont tous les multiples de 4 de $[0, 99]$ non multiples de 5.
c) Pour quels $n \geq 1$ l'écriture de 2^n se termine-t-elle par 76 ? Peut-elle se terminer par 50 ou par 06 ?

Exercice 41 Anagrammes de puissances de 2 ★★★

corrigé p. 55

Deux entiers sont *anagrammes* s'ils s'écrivent avec les mêmes chiffres, répétés autant de fois, dans un autre ordre (comme 1035 et 3105). $S(N)$ est la somme des chiffres de N .

1. Montrer que deux anagrammes sont congrus modulo 9.
2. a) Dresser le tableau des restes de 2^n modulo 9 pour $0 \leq n \leq 6$; en déduire que, pour $m, n \in \mathbb{N}$: $2^m \equiv 2^n$ [9] $\iff m \equiv n$ [6].
b) Montrer que $S(2^n)$ n'est jamais un multiple de 3. Peut-il valoir 2025 ?
3. On suppose que 2^m et 2^n sont anagrammes, avec $m > n$. a) Montrer que $2^m < 10 \times 2^n$, puis que $m - n \leq 3$. b) Conclure.

- Montrer de même que deux puissances de 5 distinctes ne sont jamais anagrammes.
- Vérifier que $3105 = 3 \times 1035$. Pourquoi la méthode ne dit-elle rien pour les puissances de 3 ?

Exercice 42 Codes-barres et clés de contrôle ★★★

corrigé p. 55

Un code-barres EAN-13 a 13 chiffres $a_1 \dots a_{13}$ (au Maroc, il commence par 611); la clé a_{13} est choisie pour que $S = a_1 + 3a_2 + a_3 + 3a_4 + \dots + 3a_{12} + a_{13} \equiv 0 [10]$. Si $S \not\equiv 0 [10]$, le lecteur signale une erreur.

- Calculer la clé du code dont les douze premiers chiffres sont 6 1 1 1 2 0 2 6 0 5 1 7.
- a) Dresser le tableau des restes de $3x$ modulo 10 pour $0 \leq x \leq 9$. b) Un seul chiffre a_i est mal lu et remplacé par $b \neq a_i$. Montrer que S est modifié de $w(b - a_i)$, avec $w \in \{1, 3\}$, et que l'erreur est toujours détectée.
- On échange deux chiffres voisins distincts $x = a_i$ et $y = a_{i+1}$. Montrer que S varie de $\pm 2(x - y)$ et que l'erreur est détectée si et seulement si $|x - y| \neq 5$. Exemple d'échange non détecté dans le code de 1 ?
- Un ISBN-10 (livres) a 10 chiffres $a_1 \dots a_{10}$ tels que $\sum_{k=1}^{10} k a_k \equiv 0 [11]$ (le dernier peut valoir 10, noté X). Montrer que l'échange de deux chiffres distincts a_i et a_j ($i < j$), voisins ou non, est toujours détecté.

22**Nombres premiers**

Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, il a $d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$ diviseurs positifs, de somme $\sigma(n) = \prod \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$.

Exercice 43 Premier ou composé ? ★

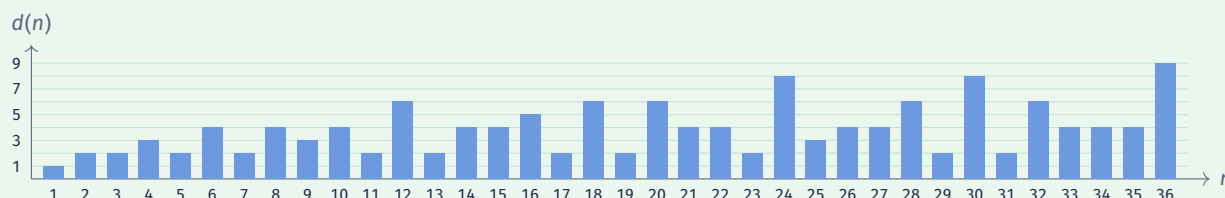
corrigé p. 56

- À l'aide du critère du cours (un entier $n \geq 2$ sans diviseur premier $p \leq \sqrt{n}$ est premier), montrer que 487 est premier et que 779 ne l'est pas.
- Écrire chacun des entiers 899, 1599 et 9991 comme une différence de deux carrés $a^2 - b^2$ (chercher a juste au-dessus de $\sqrt{n}$), puis le décomposer en facteurs premiers.
- Vérifier que $1\,000\,027 = 100^3 + 3^3$, puis, avec $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$, décomposer $1\,000\,027$ en facteurs premiers.

Exercice 44 Le diagramme des diviseurs ★

corrigé p. 56

Le diagramme donne le nombre $d(n)$ de diviseurs positifs de n , pour $1 \leq n \leq 36$.



- Lire les entiers n tels que $d(n) = 2$; justifier que $d(n) = 2$ si et seulement si n est premier.
- Lire les n tels que $d(n) = 3$, puis tels que $d(n) = 5$. Montrer que $d(n) = 3 \iff n = p^2$ et $d(n) = 5 \iff n = p^4$ (p premier). Quel est le plus petit entier ayant exactement 5 diviseurs après 16 ?

3. Montrer que $d(n) = 4$ si et seulement si $n = p^3$ ou $n = pq$ (p, q premiers distincts). Lister les entiers $n \leq 36$ tels que $d(n) = 4$ et contrôler sur le diagramme. Quel entier $n \leq 36$ a le plus de diviseurs ?

Exercice 45 Compter les diviseurs ★★

corrigé p. 57

- Décomposer $N = 2160$. Combien N a-t-il de diviseurs positifs ? pairs ? impairs ? multiples de 30 ? carrés parfaits ? Calculer la somme des diviseurs impairs de N .
- Soit $n = 2^a m$ avec $a \in \mathbb{N}$ et m impair. Montrer que $d(2n) - d(n) = d(m)$, qui est le nombre de diviseurs impairs de n . Vérifier avec $n = 2160$.
- Déterminer les entiers $n = 2^a 3^b$ ($a, b \in \mathbb{N}$) tels que $2n$ ait 4 diviseurs de plus que n , et $3n$ en ait 6 de plus que n .

Exercice 46 Autour des premiers jumeaux ★★

corrigé p. 57

Deux nombres premiers sont *jumeaux* s'ils diffèrent de 2 (par exemple 11 et 13).

- Soient p et $p + 2$ deux premiers jumeaux, avec $p \geq 5$. Montrer que $p \equiv 5 [6]$, puis que 12 divise leur somme.
- Déterminer les nombres premiers p tels que $p^2 + 4$ et $p^2 + 6$ soient aussi premiers (raisonner modulo 5).
- Soient $p < q$ deux nombres premiers. Montrer que $pq + 1$ est un carré parfait si et seulement si p et q sont jumeaux. Pour quels premiers p l'entier $5p + 1$ est-il un carré ? et $23p + 1$?

Exercice 47 Les nombres amiables ★★★

corrigé p. 57

Deux entiers distincts a et b sont *amiables* si chacun est la somme des diviseurs de l'autre, celui-ci exclu : $\sigma(a) - a = b$ et $\sigma(b) - b = a$ ($\sigma(n)$: somme des diviseurs positifs de n).

- Montrer que $a \neq b$ sont amiables si et seulement si $\sigma(a) = \sigma(b) = a + b$. Vérifier que 220 et 284 sont amiables (couple connu des Pythagoriciens).
- Règle de Thābit ibn Qurra* (Bagdad, IX^e siècle). Soit $n \geq 2$; on pose $p = 3 \times 2^{n-1} - 1$, $q = 3 \times 2^n - 1$, $r = 9 \times 2^{2n-1} - 1$, et l'on suppose p, q, r premiers.
 - Montrer que p, q, r sont impairs et que $p < q < r$.
 - Montrer que $\sigma(2^n pq) = \sigma(2^n r) = 9 \times 2^{2n-1} (2^{n+1} - 1)$.
 - Montrer que $2^n pq + 2^n r$ est égal au même nombre, et conclure que $A = 2^n pq$ et $B = 2^n r$ sont amiables.
- Retrouver le couple de la question 1 avec $n = 2$.
 - Pourquoi la règle ne s'applique-t-elle pas pour $n = 3$?
 - Pour $n = 4$, montrer que $r = 1151$ est premier et en déduire un nouveau couple d'amiables (connu du savant marakchi Ibn al-Bannā' vers 1300, retrouvé par Fermat en 1636).

Exercice 48 Premiers de la forme $6k - 1$ et $4k + 3$ ★★★

corrigé p. 58

Tout premier $p \geq 5$ vérifie $p \equiv 1$ ou $5 [6]$ (cours). On montre qu'il existe une infinité de premiers $p \equiv 5 [6]$, de la forme $6k - 1$.

- Montrer qu'un produit d'entiers tous congrus à 1 modulo 6 est congru à 1 modulo 6.

- Soit $N \geq 2$ tel que $N \equiv 5 \pmod{6}$. a) Montrer que $2 \nmid N$ et $3 \nmid N$. b) À l'aide de la décomposition de N , montrer que N a un diviseur premier $p \equiv 5 \pmod{6}$.
- Soit $n \geq 3$ et $N = n! - 1$. a) Montrer que $N \equiv 5 \pmod{6}$ et que tout diviseur premier de N est strictement supérieur à n . b) En déduire qu'il existe un nombre premier de la forme $6k - 1$ supérieur à n , puis qu'il en existe une infinité.
- Adapter la méthode à la forme $4k + 3$ ($n \geq 4$; illustrer avec $5! - 1 = 119$). Pourquoi échoue-t-elle pour la forme $6k + 1$ (penser à 5×11) ?

23

PGCD et PPCM

Pour un PGCD : l'algorithme d'Euclide ($a \wedge b = b \wedge r$) ou la décomposition (plus petits exposants) ; pour un PPCM : $(a \wedge b)(a \vee b) = |ab|$ ou les plus grands exposants. Devant un système, on écrit $a = da'$, $b = db'$ avec $d = a \wedge b$ et $a' \wedge b' = 1$.

Exercice 49 L'algorithme d'Euclide en tableau ★

corrigé p. 59

On pose $a = 7470$ et $b = 4770$.

- Effectuer l'algorithme d'Euclide en présentant les divisions successives dans un tableau ; en déduire $d = a \wedge b$.
- En déduire $a \vee b$, puis la forme irréductible de la fraction $\frac{b}{a}$.
- Décomposer a et b en produits de facteurs premiers et retrouver d et $a \vee b$.
- Combien a et b ont-ils de diviseurs communs dans $\mathbb{N}$? dans $\mathbb{Z}$? Écrire les diviseurs communs positifs.
- a) Déterminer le plus petit entier $k \geq 1$ tel que ka soit un carré parfait. b) Déterminer le plus petit entier $n \geq 1$ tel que b divise na ; comparer na et $a \vee b$.

Exercice 50 Retrouver deux entiers ★

corrigé p. 59

Dans chaque cas, déterminer les couples (a, b) d'entiers naturels non nuls, avec $a \leq b$, tels que :

- $a \wedge b = 14$ et $ab = 11760$;
- $a \vee b = 10(a \wedge b)$ et $a + b = 189$;
- $a \wedge b = 6$ et $b^2 - a^2 = 756$.

Exercice 51 Une fraction qui dépend de n ★★

corrigé p. 60

Pour $n \in \mathbb{Z}$, on pose $A = 2n + 1$, $B = n^2 + 6n + 11$ et $d = A \wedge B$ (on remarque que $A \neq 0$).

- Vérifier que $4B - (2n + 1)A = 33$. En déduire que d divise 33.
- a) Montrer que $3 \mid A \iff n \equiv 1 \pmod{3}$, et que dans ce cas $3 \mid B$. b) Montrer que $11 \mid A \iff n \equiv 5 \pmod{11}$, et que dans ce cas $11 \mid B$. c) En déduire la valeur de d selon n , puis d pour $n = 5, 16, 2026$ et 2027 .
- Pour quels entiers n la fraction $\frac{B}{A}$ est-elle irréductible ?
- Déterminer les entiers relatifs n pour lesquels $\frac{B}{A}$ est un entier.

Exercice 52 Fractions irréductibles de dénominateur n ★★

corrigé p. 60

Soit $n \geq 2$. On note I_n l'ensemble des entiers k tels que $1 \leq k \leq n-1$ et $k \wedge n = 1$ (la fraction $\frac{k}{n}$ est alors irréductible), N_n le nombre d'éléments de I_n et S_n la somme des fractions $\frac{k}{n}$ pour $k \in I_n$.

1. Montrer que $k \wedge n = (n-k) \wedge n$ pour tout $k \in \mathbb{Z}$, puis que $k \in I_n \iff n-k \in I_n$.
2. On suppose $n \geq 3$. Montrer que $k \neq n-k$ pour tout $k \in I_n$. En déduire que N_n est pair et que $S_n = \frac{N_n}{2}$.
3. Soit p un nombre premier et $a \geq 1$ (avec $p^a \geq 3$). Montrer que $N_{p^a} = p^a - p^{a-1}$. Calculer N_n et S_n pour $n = 1024$ et pour $n = 343$.
4. Soit $p \neq q$ deux nombres premiers. Montrer que $N_{pq} = (p-1)(q-1)$. Application : $n = 2026$ (vérifier que 1013 est premier) et $n = 2021 = 43 \times 47$.

Exercice 53 Somme et PPCM ★★★

corrigé p. 61

1. Soit $a', b' \in \mathbb{N}^*$ premiers entre eux. Montrer par l'absurde que $(a' + b') \wedge (a'b') = 1$.
2. Soit $a, b \in \mathbb{N}^*$. En déduire que $(a+b) \wedge (a \vee b) = a \wedge b$.
3. a) Déterminer les couples $(a, b) \in \mathbb{N}^{*2}$ tels que $a+b = 276$ et $a \vee b = 1440$. b) Montrer qu'aucun couple ne vérifie $a+b = 60$ et $a \vee b = 84$.
4. a) Soit $a, b \in \mathbb{N}^*$. Montrer que si $\frac{a}{b} + \frac{b}{a}$ est un entier, alors $a = b$. b) En déduire les rationnels $x \neq 0$ tels que $x + \frac{1}{x} \in \mathbb{Z}$.

Exercice 54 PGCD et PPCM de trois entiers ★★★

corrigé p. 61

Pour $a \in \mathbb{N}^*$ et p premier, $v_p(a)$ désigne l'exposant de p dans la décomposition de a ($v_p(a) = 0$ si $p \nmid a$) ; on sait que $v_p(a \wedge b) = \min(v_p(a), v_p(b))$ et $v_p(a \vee b) = \max(v_p(a), v_p(b))$. Pour $a, b, c \in \mathbb{N}^*$, on pose $a \wedge b \wedge c = (a \wedge b) \wedge c$ et $a \vee b \vee c = (a \vee b) \vee c$.

1. Montrer que $v_p(a \wedge b \wedge c) = \min(v_p(a), v_p(b), v_p(c))$ et $v_p(a \vee b \vee c) = \max(v_p(a), v_p(b), v_p(c))$. En déduire que $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et que les diviseurs communs à a, b, c sont les diviseurs de $a \wedge b \wedge c$.
2. Montrer que, pour tous réels x, y, z : $\max(x, y, z) + \min(x, y) + \min(y, z) + \min(z, x) = x + y + z + \min(x, y, z)$.
3. En déduire que $(a \vee b \vee c) \times (a \wedge b)(b \wedge c)(c \wedge a) = abc \times (a \wedge b \wedge c)$.
4. Calculer $40 \vee 56 \vee 140$ à l'aide de 3, les PGCD étant obtenus par l'algorithme d'Euclide ; vérifier par la décomposition.
5. Montrer que $a \vee b \vee c = abc$ si et seulement si a, b, c sont premiers entre eux deux à deux. Calculer $6 \wedge 10 \wedge 15$ et $6 \vee 10 \vee 15$: conclusion ?
6. Montrer que $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$.

24

Équations en nombres entiers

Trois réflexes : **factoriser** pour se ramener à $uv = n$ (on parcourt alors les diviseurs de n) ; **étudier les restes** modulo un entier bien choisi (pour prouver une impossibilité ou réduire les cas) ; **encadrer** (pour qu'il ne reste qu'un nombre fini de cas). On vérifie toujours les solutions trouvées.

Exercice 55 Factoriser pour résoudre ★

corrigé p. 62

- Vérifier que $xy + x + y + 1 = (x + 1)(y + 1)$, puis résoudre dans $\mathbb{N}^2$: $xy + x + y = 41$.
- Résoudre dans $\mathbb{Z}^2$: $xy = 3x + 5y + 1$ (écrire l'équation sous la forme $(x - 5)(y - 3) = k$).

- Un jardin rectangulaire de dimensions entières $x \leq y$ (en mètres) est entouré d'une allée de 1 m de large (figure) ; l'aire de l'allée est égale à celle du jardin. Montrer que $(x - 2)(y - 2) = 8$ et trouver les dimensions possibles du jardin.



Exercice 56 Différences de carrés ★

corrigé p. 63

- Résoudre dans $\mathbb{N}^2$: $x^2 - y^2 = 105$.
- Déterminer les triangles rectangles dont les trois côtés sont des entiers et dont un côté de l'angle droit mesure 20 (on note y l'autre côté de l'angle droit et x l'hypoténuse).
- Résoudre dans $\mathbb{Z}^2$: $x^2 - 4y^2 = 33$.

Exercice 57 Le bon modulo ★★

corrigé p. 63

- a) Dresser la table des restes de y^2 et de $3y^2$ modulo 5. b) Montrer que l'équation $15x^2 - 7y^2 = 9$ n'a aucune solution dans $\mathbb{Z}^2$.
- a) Montrer que $4^3 \equiv 1 [21]$ et en déduire le reste de 4^x modulo 21 selon le reste de x modulo 3.
b) Montrer que l'équation $4^x - 21y = 5$ n'a aucune solution $(x, y) \in \mathbb{N} \times \mathbb{Z}$. c) Résoudre dans $\mathbb{N} \times \mathbb{Z}$: $4^x - 21y = 16$.
- On veut résoudre dans $\mathbb{N}^2$ l'équation $x^2 + 3y^2 = 84$. a) Montrer que $3 \mid x$; on pose $x = 3u$. b) Montrer que $y^2 \leq 28$ et que $3 \nmid y$. c) Conclure.

Exercice 58 Le problème des cent volailles ★★

corrigé p. 63

Un manuel chinois du V^e siècle (Zhang Qiujian) pose ce problème : « Un coq coûte 5 pièces, une poule 3 pièces, et trois poussins coûtent 1 pièce. Avec 100 pièces, on achète 100 volailles. Combien de coqs, de poules et de poussins ? »

- On note x, y, z les nombres de coqs, de poules et de poussins. Montrer que $x + y + z = 100$ et $15x + 9y + z = 300$, puis que $7x + 4y = 100$.
- a) Montrer que si $7x + 4y = 100$, alors $3x \equiv 0 [4]$, puis, par un tableau de restes, que $x \equiv 0 [4]$.
b) Résoudre dans $\mathbb{N}^2$ l'équation $7x + 4y = 100$. c) Répondre au problème.
- On veut résoudre dans $\mathbb{Z}^2$ l'équation $8x - 11y = 5$. a) Montrer que $8x \equiv 5 [11]$ et en déduire, par un tableau de restes, le reste de x modulo 11. b) En déduire toutes les solutions.

4. Montrer que le reste de $12x$ modulo 18 ne dépend que du reste de x modulo 3. Pour quels entiers b la congruence $12x \equiv b \pmod{18}$ a-t-elle des solutions ? Résoudre $12x \equiv 6 \pmod{18}$.

Exercice 59 Ordonner et encadrer ★★★

corrigé p. 64

1. Un pavé droit a des arêtes de longueurs entières $x \leq y \leq z$ (en cm). Si l'on augmente chaque arête de 1 cm, son volume double. On cherche les dimensions possibles.
- a) Montrer que $\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right)\left(1 + \frac{1}{z}\right) = 2$. b) Montrer que $2 \leq \left(1 + \frac{1}{x}\right)^3$, puis que $x \in \{2, 3\}$.
- c) Traiter le cas $x = 2$ (montrer que $(y - 3)(z - 3) = 12$), puis le cas $x = 3$, et conclure.
2. Résoudre dans $\mathbb{N}^4$: $x! + y! + z! = w!$ (on supposera $x \leq y \leq z$; montrer que $w \geq z + 1$, puis que $z \leq 2$).

Exercice 60 Puissances et carrés ★★★

corrigé p. 64

1. On cherche les couples $(x, y) \in \mathbb{N}^2$ tels que $5^x - 4^y = 1$.
- a) Montrer que $x \geq 1$ et $y \geq 1$. b) En raisonnant modulo 3, montrer que x est impair.
- c) Montrer que $5^x - 1 = 4S$ avec $S = 1 + 5 + 5^2 + \dots + 5^{x-1}$, et que S est impair. Conclure.
2. Soit $P(n) = n^4 + n^3 + n^2 + n + 1$, pour $n \in \mathbb{Z}$.
- a) Vérifier que $4P(n) - (2n^2 + n)^2 = 3n^2 + 4n + 4$ et $4P(n) - (2n^2 + n + 1)^2 = -(n - 3)(n + 1)$.
- b) En déduire que si $n < -1$ ou $n > 3$, le nombre $4P(n)$ est strictement compris entre deux carrés d'entiers consécutifs.
- c) Déterminer les entiers n pour lesquels $P(n)$ est un carré parfait.

25

Défis de concours

Ces problèmes, dans l'esprit des concours et des olympiades, combinent plusieurs outils du chapitre (restes, décomposition, PGCD, encadrement) et demandent un raisonnement soigné (absurde, récurrence, tiroirs, descente).

Exercice 61 Presque une puissance de 2 ★★★★★

corrigé p. 65

On cherche les couples $(x, n) \in \mathbb{N}^2$ tels que $x^2 + 615 = 2^n$.

1. Montrer que $n \geq 10$ et que x est impair.
2. En raisonnant modulo 3, montrer que n est pair. On pose $n = 2m$.
3. Montrer que $(2^m - x)(2^m + x) = 615$, décomposer 615 et en déduire toutes les solutions.
4. Résoudre de même, dans $\mathbb{N}^2$: $x^2 + 63 = 2^n$.

Exercice 62 $n + 1$ entiers choisis parmi $1, 2, \dots, 2n$ ★★★★★

corrigé p. 65

Soit $n \geq 1$ et A une partie de $\{1, 2, \dots, 2n\}$ ayant $n + 1$ éléments (problème d'Erdős).

1. a) En considérant les n « tiroirs » $\{1, 2\}, \{3, 4\}, \dots, \{2n-1, 2n\}$, montrer que A contient deux entiers consécutifs.
- b) En déduire que A contient deux entiers premiers entre eux.

2. a) Montrer que tout entier $k \geq 1$ s'écrit de façon unique $k = 2^\alpha m$, avec $\alpha \in \mathbb{N}$ et m impair (la « partie impaire » de k).
b) En considérant les parties impaires des éléments de A , montrer que A contient deux entiers distincts dont l'un divise l'autre, et même dont le quotient est une puissance de 2.
3. Montrer que ces deux résultats deviennent faux si A n'a que n éléments.
4. On choisit 1014 entiers distincts entre 1 et 2026. Que peut-on affirmer ? Et si l'on n'en choisit que 1013 ?

Exercice 63 Le carré de son nombre de diviseurs ★★★★★

corrigé p. 66

Pour $n \in \mathbb{N}^*$, on note $d(n)$ le nombre de diviseurs positifs de n . On cherche les entiers $n \geq 1$ tels que $n = d(n)^2$.

1. Montrer par récurrence que $3^a \geq 2a + 1$ pour tout $a \in \mathbb{N}$, avec égalité si et seulement si $a \in \{0, 1\}$.
Montrer que si $p \geq 5$ est premier et $a \geq 1$, alors $p^a > 2a + 1$.
2. Soit $n \geq 2$ tel que $n = d(n)^2$. a) Montrer que n s'écrit $n = p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$ (p_i premiers distincts, $a_i \geq 1$), puis que $d(n)$ est impair et que n est impair.
b) Montrer que l'égalité $n = d(n)^2$ équivaut à $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} = (2a_1 + 1)(2a_2 + 1) \dots (2a_k + 1)$.
3. Conclure : déterminer tous les entiers $n \geq 1$ tels que $n = d(n)^2$.

Exercice 64 Nombres premiers sous contraintes ★★★★★

corrigé p. 66

1. Déterminer les triplets (p, q, r) de nombres premiers, avec $p \leq q \leq r$, tels que $pqr = 5(p + q + r)$.
2. Déterminer les couples (p, q) de nombres premiers tels que $p^q + q^p$ soit un nombre premier.
3. Déterminer les nombres premiers p tels que $p^2 + 11$ ait exactement 6 diviseurs positifs.

Exercice 65 Le saut de Viète ★★★★★

corrigé p. 67

Pour un entier k , on considère l'équation $(E_k): a^2 + b^2 + 1 = kab$, d'inconnue $(a, b) \in \mathbb{N}^{*2}$.

1. Montrer que $(1, 1)$ est solution de (E_3) . Montrer que si (E_k) a une solution (a, b) , alors $k \geq 3$ et $a \wedge b = 1$.
2. On suppose que (E_k) a des solutions, et l'on en choisit une, (a, b) , avec $a \geq b$ et $a + b$ **minimal**.
a) On pose $a' = kb - a$. Montrer que $aa' = b^2 + 1$, puis que (a', b) est encore solution de (E_k) , avec $a' \in \mathbb{N}^*$.
b) Montrer, par l'absurde, que $a = b$ (si $a \geq b + 1$, comparer a' et b). c) En déduire que $a = b = 1$ et $k = 3$.
3. Montrer que si (a, b) est solution de (E_3) avec $a \leq b$, alors $(b, 3b - a)$ en est une autre, avec $3b - a > b$. En partant de $(1, 1)$, écrire cinq solutions et montrer que (E_3) en a une infinité.

Exercice 66 Les zéros de $n!$ ★★★★★

corrigé p. 67

Pour $n \in \mathbb{N}^*$, on note $Z(n)$ le nombre de zéros qui terminent l'écriture décimale de $n!$. On admet la formule de Legendre : l'exposant de 5 dans $n!$ vaut $E\left(\frac{n}{5}\right) + E\left(\frac{n}{25}\right) + E\left(\frac{n}{125}\right) + \dots$ (somme finie), et de même pour 2.

1. Montrer que $Z(n)$ est égal à l'exposant de 5 dans $n!$.
2. a) Soit $q \in \mathbb{N}^*$ et $0 \leq r \leq 4$. En comptant des multiples, montrer que $E\left(\frac{5q+r}{5^j}\right) = E\left(\frac{q}{5^{j-1}}\right)$ pour $j \geq 1$, puis que $Z(5q+r) = q + Z(q)$.
b) En déduire que Z est croissante, et que chaque valeur prise par Z l'est exactement 5 fois (sauf la valeur 0). c) Montrer que $Z(n) < \frac{n}{4}$.
3. a) Calculer $Z(8120)$, $Z(8119)$ et $Z(8125)$. b) Déterminer les entiers n tels que $n!$ se termine par exactement 2026 zéros.
c) Montrer qu'aucune factorielle ne se termine par exactement 2027, 2028 ou 2029 zéros.

Partie D • Corrigés

Des solutions détaillées, rédigées comme sur une copie

26

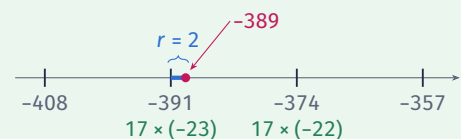
Corrigés du niveau I

■ Corrigé de l'exercice 1

1. On cherche les entiers d tels que $-20 = dk$ avec $k \in \mathbb{Z}$: ce sont les diviseurs positifs de 20 (1, 2, 4, 5, 10, 20) et leurs opposés. $D(-20) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20\}$: 12 éléments.
2. a) **Vrai** : $91 = (-7) \times (-13)$. b) **Vrai** : $-84 = 12 \times (-7)$. c) **Faux** : $0 \times k = 0 \neq 6$ pour tout $k \in \mathbb{Z}$ (0 ne divise que 0). d) **Vrai** : $0 = 9 \times 0$. e) **Faux** : $-5 = 15k$ donnerait $k = -\frac{1}{3} \notin \mathbb{Z}$. f) **Vrai** : $45 = 9 \times 5 = 15 \times 3$.
3. Un diviseur commun divise toute combinaison $u(4n+7) + v(3n+5)$ ($u, v \in \mathbb{Z}$). On choisit $u = 3$, $v = -4$ pour éliminer n : $3(4n+7) - 4(3n+5) = 21 - 20 = 1$. Donc $d \mid 1$, et $d = 1$ ou $d = -1$.
4. a) On fait disparaître n : $3n+5 = 3(n+4) - 7$. Si $n+4 \mid 3n+5$, alors $n+4 \mid 3(n+4) - (3n+5) = 7$; réciproquement, si $n+4 \mid 7$, alors $n+4 \mid 3(n+4) - 7 = 3n+5$. Donc $n+4 \mid 3n+5 \iff n+4 \in \{-7, -1, 1, 7\} \iff n \in \{-11, -5, -3, 3\}$.
b) **Analyse**. Si $2n+1 \mid n+7$, alors $2n+1 \mid 2(n+7) - (2n+1) = 13$: $2n+1 \in \{-13, -1, 1, 13\}$, soit $n \in \{-7, -1, 0, 6\}$. **Synthèse** (on n'a qu'une implication : on vérifie chaque candidat) : $n = -7$: $-13 \mid 0$; $n = -1$: $-1 \mid 6$; $n = 0$: $1 \mid 7$; $n = 6$: $13 \mid 13$. $n \in \{-7, -1, 0, 6\}$.

■ Corrigé de l'exercice 2

1. On encadre a entre deux multiples consécutifs de $|b|$, le reste étant toujours positif. a) $17 \times 22 = 374 \leq 389 < 391$: $389 = 17 \times 22 + 15$. b) $17 \times (-23) = -391 \leq -389 < -374$: $-389 = 17 \times (-23) + 2$ (et non $17 \times (-22) - 15$: un reste n'est jamais négatif). c) $389 = (-17) \times (-22) + 15$. d) $-389 = (-17) \times 23 + 2$. Enfin $\frac{-389}{17} \approx -22,9$, donc $E\left(\frac{-389}{17}\right) = -23 = q$ ✓.
2. Le quotient vaut 7 si et seulement si $100 = 7n + r$ avec $0 \leq r < n$: $0 \leq 100 - 7n < n \iff 7n \leq 100 < 8n \iff 12,5 < n \leq \frac{100}{7} \approx 14,3$. $n = 13$ (reste 9) ou $n = 14$ (reste 2).
3. On écrit $a = 6q + 4$ et on fait apparaître la forme $6q' + r'$ avec $0 \leq r' \leq 5$. $-a = 6(-q-1) + 2$: reste 2 ; $2a = 6(2q+1) + 2$: reste 2 ; $a^2 = 36q^2 + 48q + 16 = 6(6q^2 + 8q + 2) + 4$: reste 4 ; $a = 3(2q+1) + 1$: reste 1 dans la division par 3.



■ Corrigé de l'exercice 3

1. a) **Disjonction des cas selon la parité de n .** Si n est pair, $n + 2$ est pair ; si n est impair, $n + 5$ est pair. Dans les deux cas, $(n + 2)(n + 5)$ est **pair**. b) $n^2 + n = n(n + 1)$ est le produit de deux entiers consécutifs, donc pair : $n^2 + n + 1$ est **impair**.

2. **Le reste d'un produit par 3 se lit sur les restes des facteurs** (compatibilité avec $+$ et $\times$) : dans le tableau ci-contre, chaque colonne contient un facteur de reste 0. Dans tous les cas, l'un des trois facteurs est divisible par 3 : $\boxed{3 \mid n(n + 4)(2n + 1)}$.

reste de n	0	1	2
n	0	1	2
$n + 4$	1	2	0
$2n + 1$	1	0	2
produit	0	0	0

3. a) Si $n = 10q + r$ ($0 \leq r \leq 9$), alors $n(n + 1) = 100q^2 + 10q(2r + 1) + r(r + 1)$: **le reste de $n(n + 1)$ par 10 est celui de $r(r + 1)$.**

r	0	1	2	3	4	5	6	7	8	9
$r(r + 1)$	0	2	6	12	20	30	42	56	72	90
reste par 10	0	2	6	2	0	0	2	6	2	0

Restes possibles : $\boxed{0, 2, 6}$.

- b) Le chiffre des unités de $n^2 + n + 1$ est son reste par 10, c'est-à-dire celui de $n(n + 1) + 1$: $\boxed{1, 3 \text{ ou } 7}$.

■ Corrigé de l'exercice 4

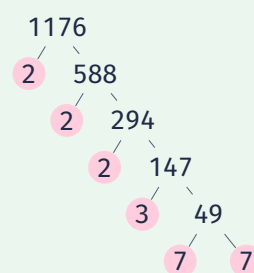
1. $a \equiv b [n] \iff n \mid a - b$. a) $47 - 5 = 42 = 7 \times 6$: **vrai**. b) $-13 - 8 = -21$: **vrai**. c) $100 - (-1) = 101$: **vrai**. d) $2026 - 2 = 2024$ n'est pas multiple de 5 : **faux** ($2026 \equiv 1 [5]$). e) $38 + 2 = 40$ n'est pas multiple de 9 : **faux** ($38 \equiv 2 [9]$).
2. **Compatibilité avec $+$, $\times$ et les puissances : on remplace a par 3 et b par 5.** $a + b \equiv 8 \equiv \boxed{1}$; $ab \equiv 15 \equiv \boxed{1}$; $a - b \equiv -2 \equiv \boxed{5}$; $a^2 + b^2 \equiv 34 \equiv \boxed{6}$; $a^3 \equiv 27 \equiv \boxed{6}$; $2a - 3b + 1 \equiv -8 \equiv \boxed{6}$ (restes par 7).
3. $27 = 2 \times 13 + 1$: $3^3 \equiv 1 [13]$. Comme $1000 = 3 \times 333 + 1$: $3^{1000} = (3^3)^{333} \times 3 \equiv 1 \times 3$: reste $\boxed{3}$. Et $29 = 2 \times 13 + 3 \equiv 3 [13]$: $29^{1000} \equiv 3^{1000}$: reste $\boxed{3}$.
4. **Une congruence modulo n ne dépend que du reste r de x : on teste $r = 0, \dots, n - 1$.** a) $x \equiv 1 - 4 = -3 \equiv 3 [6]$: $\boxed{x = 3 + 6k, k \in \mathbb{Z}}$. b) $3r$ modulo 7 vaut 0, 3, 6, 2, 5, 1, 4 pour $r = 0, \dots, 6$: $\boxed{x \equiv 3 [7]}$. c) $4r$ modulo 6 vaut 0, 4, 2, 0, 4, 2 : $r \in \{2, 5\}$, $\boxed{x \equiv 2 [3]}$. d) r^2 modulo 5 vaut 0, 1, 4, 4, 1 : $\boxed{x \equiv 2 \text{ ou } 3 [5]}$. e) $2x - 1$ est impair, il n'est jamais multiple de 4 : **aucune solution**.

■ Corrigé de l'exercice 5

1. **Critère : si $n \geq 2$ n'a aucun diviseur premier $p \leq \sqrt{n}$, alors n est premier.** $253 = 11 \times 23$; $299 = 13 \times 23$; $361 = 19^2$; $377 = 13 \times 29$: **composés**. $257 : 16^2 < 257 < 17^2$, et 257 n'est divisible ni par 2, 3 (somme 14), 5, ni par 7, 11, 13 (restes 5, 4, 10) : **premier**. $307 : 17^2 < 307 < 19^2$; restes par 7, 11, 13, 17 : 6, 10, 8, 1 (et ni 2, ni 3, ni 5) : **premier**. $409 : 20^2 < 409 < 21^2$; restes par 7, 11, 13, 17, 19 : 3, 2, 6, 1, 10 : **premier**. **Premiers : 257, 307, 409.**
2. a) p est impair, donc $\frac{p+1}{2}$ sont des entiers, et $\left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 = \frac{(p+1)^2 - (p-1)^2}{4} = \frac{4p}{4} = p$.
b) **Analyse.** Si $p = x^2 - y^2 = (x - y)(x + y)$ avec $x, y \in \mathbb{N}$: $x + y \geq 0$ et le produit est positif, donc $x + y > 0$ et $x - y > 0$, avec $x - y \leq x + y$. Les seuls diviseurs positifs de p étant 1 et p : $x - y = 1$ et $x + y = p$, d'où $x = \frac{p+1}{2}$ et $y = \frac{p-1}{2}$: l'écriture est **unique**. c) $\boxed{409 = 205^2 - 204^2}$.

■ Corrigé de l'exercice 6

- Divisions successives par les nombres premiers croissants** (arbre ci-contre pour A) : $A = 2^3 \times 3 \times 7^2$; $1260 = 2 \times 630 = 2^2 \times 315 = 2^2 \times 3^2 \times 35$; $B = 2^2 \times 3^2 \times 5 \times 7$.
- Un entier $\prod p^\alpha$ a $\prod (\alpha + 1)$ diviseurs positifs**, et deux fois plus dans $\mathbb{Z}$ (les opposés). A : $(3 + 1)(1 + 1)(2 + 1) = 24$ dans $\mathbb{N}$, 48 dans $\mathbb{Z}$.
B : $3 \times 3 \times 2 \times 2 = 36$ dans $\mathbb{N}$, 72 dans $\mathbb{Z}$.
- PGCD : plus petits exposants ; PPCM : plus grands exposants**. $A \wedge B = 2^2 \times 3 \times 7 = 84$; $A \vee B = 2^3 \times 3^2 \times 5 \times 7^2 = 17\,640$. $84 \times 17\,640 = 1\,481\,760 = 1176 \times 1260$ ✓.
- Un carré parfait est un entier dont tous les exposants sont pairs**. Dans kA , les exposants de 2 et de 3 doivent devenir pairs : $6 \mid k$. Le plus petit est $k = 6$: $6A = 2^4 \times 3^2 \times 7^2 = 84^2 = 7056$. De même, pour B : $k = 35$, et $35B = 2^2 \times 3^2 \times 5^2 \times 7^2 = 210^2 = 44\,100$.



■ Corrigé de l'exercice 7

- Algorithme d'Euclide** : $a \wedge b = b \wedge r$; le PGCD est le dernier reste non nul.

dividende	1517	1189	328	205	123	82
diviseur	1189	328	205	123	82	41
quotient	1	3	1	1	1	2
reste	328	205	123	82	41	0

$1517 \wedge 1189 = 41$. Comme $1517 = 41 \times 37$ et $1189 = 41 \times 29$: $1517 \vee 1189 = \frac{1517 \times 1189}{41} = 37 \times 1189 =$

$43\,993$ et $\frac{1189}{1517} = \frac{29}{37}$ ($29 \wedge 37 = 1$).

- On utilise $(ka) \wedge (kb) = |k|(a \wedge b)$, et le PGCD ne dépend pas des signes**. $3034 \wedge 2378 = (2 \times 1517) \wedge (2 \times 1189) = 82$; $(-4551) \wedge 3567 = (3 \times 1517) \wedge (3 \times 1189) = 123$.
- Soit $d \geq 1$ un diviseur commun. Si $d \mid n$ et $d \mid 3n + 1$, alors $d \mid (3n + 1) - 3n = 1$: $n \wedge (3n + 1) = 1$.
Si $d \mid 2n + 1$ et $d \mid 2n + 3$, alors $d \mid 2$, donc $d \in \{1, 2\}$; or $2n + 1$ est impair : $d = 1$ et $(2n + 1) \wedge (2n + 3) = 1$.

■ Corrigé de l'exercice 8

- Critères du cours** : dernier chiffre (par 2, 5), deux derniers (par 4), trois derniers (par 8), somme des chiffres (par 3, 9), somme alternée des chiffres en partant des unités (par 11). $7\,425$: dernier chiffre 5, donc divisible par 5 mais ni par 2, ni par 4, ni par 8 ; somme 18 : divisible par 3 et par 9 ; $5 - 2 + 4 - 7 = 0$: divisible par 11 ($7\,425 = 3^3 \times 5^2 \times 11$). $123\,456$: pair ; $56 = 4 \times 14$ et $456 = 8 \times 57$: divisible par 4 et par 8 ; pas par 5 ; somme 21 : par 3, pas par 9 ; $6 - 5 + 4 - 3 + 2 - 1 = 3$: pas par 11.
- $45 = 5 \times 9$ avec $5 \wedge 9 = 1$: $45 \mid N \iff (5 \mid N \text{ et } 9 \mid N)$. $5 \mid N \iff y \in \{0, 5\}$; $9 \mid N \iff 9 \mid 10 + x + y$. Si $y = 0$: $x = 8$; si $y = 5$: $x = 3$. 3870 et 3375 .
- $99 = 9 \times 11$ avec $9 \wedge 11 = 1$. $9 \mid x + 1 + 3 + y$ et $11 \mid y - 3 + 1 - x = y - x - 2$. Comme $-11 \leq y - x - 2 \leq 6$: $y = x + 2$ ou $y - x - 2 = -11$, soit $(x, y) = (9, 0)$, exclu ($9 + 0 + 4 = 13$). Avec $y = x + 2$: $9 \mid 2x + 6$ et $8 \leq 2x + 6 \leq 20$, donc $2x + 6 = 18$: $x = 6$, $y = 8$. $6138 = 99 \times 62$.

27 Corrigés du niveau 2

■ Corrigé de l'exercice 9

1. a) $(n+3)(n+1)+6 = n^2+4n+3+6 = n^2+4n+9$. b) **On reconnaît une division euclidienne grâce à l'unicité : il suffit que le reste vérifie $0 \leq r < n+3$.** Pour $n \geq 4$: $n^2+4n+9 = (n+3)(n+1)+6$ avec $0 \leq 6 < n+3$: **quotient $n+1$, reste 6** . Pour $n = 1$: $6 \geq n+3 = 4$, ce n'est plus le cas : $14 = 4 \times 3 + 2$ (quotient 3, reste 2). c) Si $n+3$ divise n^2+4n+9 , il divise $n^2+4n+9 - (n+1)(n+3) = 6$; réciproquement, s'il divise 6, il divise $(n+1)(n+3)+6$. Donc $n+3 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$: $n \in \{-9, -6, -5, -4, -2, -1, 0, 3\}$.
2. a) **Le reste de n^2+n+7 par 9 ne dépend que du reste r de n par 9 :**
- | r | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|-------------|---|---|----|----|----|----|----|----|----|
| r^2+r+7 | 7 | 9 | 13 | 19 | 27 | 37 | 49 | 63 | 79 |
| reste par 9 | 7 | 0 | 4 | 1 | 0 | 1 | 4 | 0 | 7 |
- b) $9 \mid n^2+n+7 \iff r \in \{1, 4, 7\}$. Or $n \equiv r [3]$ et 1, 4, 7 sont exactement les restes $r \leq 8$ congrus à 1 modulo 3 : $9 \mid n^2+n+7 \iff n \equiv 1 [3]$.
- c) $n^2+n+7 = 9k^2+6k+1+3k+1+7 = 9(k^2+k+1)$. **Disjonction des cas selon le reste de k par 3.** Si $k = 3j$: $k^2+k+1 = 3(3j^2+j)+1$; si $k = 3j+2$: $k^2+k+1 = 3(3j^2+5j+2)+1$: non divisible par 3, donc pas par 9. Si $k = 3j+1$: $k^2+k+1 = 9j^2+9j+3 = 9(j^2+j)+3$: reste 3 par 9. Dans tous les cas, $9 \nmid k^2+k+1$.
- d) **Par l'absurde** : si $81 \mid n^2+n+7$, alors $9 \mid n^2+n+7$, donc $n = 3k+1$ (question b) et $81 \mid 9(k^2+k+1)$, soit $9 \mid k^2+k+1$: contradiction avec c). Donc $81 \nmid n^2+n+7$ pour tout $n \in \mathbb{Z}$.

■ Corrigé de l'exercice 10

1. a) $3^5 = 243 = 11 \times 22 + 1$: $3^5 \equiv 1 [11]$. **On divise l'exposant par la période** : si $n = 5q+r$ ($0 \leq r \leq 4$), alors $3^n = (3^5)^q 3^r \equiv 3^r [11]$.
- | reste de n par 5 | 0 | 1 | 2 | 3 | 4 |
|-----------------------|---|---|---|---|---|
| reste de 3^n par 11 | 1 | 3 | 9 | 5 | 4 |
- b) $999 = 5 \times 199 + 4$: $3^{999} \equiv 4$. $47 = 4 \times 11 + 3$, donc $47^{2027} \equiv 3^{2027}$, et $2027 = 5 \times 405 + 2$: reste 9. $3^3 = 27 = 2 \times 11 + 5$: $5^{100} \equiv 3^{300} \equiv (3^5)^{60} \equiv 1$.
- c) $11 \mid 3^n + 2 \iff 3^n \equiv -2 \equiv 9 [11] \iff n \equiv 2 [5]$, soit $n = 5k+2$ ($k \in \mathbb{N}$). De même $11 \mid 3^n + 1 \iff 3^n \equiv 10 [11]$: 10 n'est pas dans le tableau, donc $3^n + 1$ n'est **jamais** divisible par 11.
2. $256 = 11 \times 23 + 3$. **On ramène tout aux puissances de 3** : $4^{4n+2} = 16 \times (4^4)^n = 16 \times 256^n \equiv 5 \times 3^n [11]$, et $3^{n+3} = 27 \times 3^n \equiv 5 \times 3^n [11]$. Donc $3^{n+3} - 4^{4n+2} \equiv 0$: $11 \mid 3^{n+3} - 4^{4n+2}$ pour tout $n \in \mathbb{N}$.
3. $3^4 = 81 \equiv 1 [10]$ et $999 = 4 \times 249 + 3$: $3^{999} \equiv 3^3 = 27 \equiv 7 [10]$: chiffre des unités 7. **Astuce** : $7 \equiv -3 [10]$ et 999 est impair, donc $7^{999} \equiv (-3)^{999} = -3^{999} [10]$, et $3^{999} + 7^{999} \equiv 0 [10]$: $10 \mid 3^{999} + 7^{999}$.

■ Corrigé de l'exercice 11

1. a) **Algorithme d'Euclide** : $4199 = 2431 \times 1 + 1768$; $2431 = 1768 \times 1 + 663$; $1768 = 663 \times 2 + 442$; $663 = 442 \times 1 + 221$; $442 = 221 \times 2 + 0$. Dernier reste non nul : $4199 \wedge 2431 = 221$. Comme $4199 = 221 \times 19$ et $2431 = 221 \times 11$: $4199 \vee 2431 = 221 \times 19 \times 11 = 46\,189$. b) $\frac{2431}{4199} = \frac{11}{19}$.
2. a) **On divise b par a** : $b = n^2+5n+15 = (n+4)(n+1)+11$. Si $d \mid a$ et $d \mid b$, alors $d \mid b - (n+1)a = 11$; si $d \mid a$ et $d \mid 11$, alors $d \mid (n+1)a + 11 = b$. Les diviseurs communs de a et b sont ceux de a et 11 : $a \wedge b = a \wedge 11$.

b) 11 est premier : $a \wedge 11 \in \{1, 11\}$, et $a \wedge b = 11 \iff 11 \mid n + 4 \iff n \equiv -4 \equiv 7 [11]$.
 $a \wedge b \in \{1, 11\}$; $\frac{b}{a}$ est irréductible $\iff a \wedge b = 1 \iff n \not\equiv 7 [11]$. c) $n = 18 \equiv 7 [11]$:
 $a = 22 = 2 \times 11$, $b = 429 = 3 \times 11 \times 13$, $a \wedge b = 11$ ✓.

3. On écrit $a = 21a'$, $b = 21b'$ avec $a' \wedge b' = 1$ (cours) ; alors $a \vee b = 21a'b'$. Donc $a'b' = \frac{2310}{21} = 110 = 2 \times 5 \times 11$, avec $a' \leq b'$ et $a' \wedge b' = 1$: chaque facteur premier va entièrement dans a' ou dans b' : $(a', b') \in \{(1, 110), (2, 55), (5, 22), (10, 11)\}$. Solutions : $(21, 2310)$, $(42, 1155)$, $(105, 462)$, $(210, 231)$. $a + b = 21(a' + b') = 441 \iff a' + b' = 21$: $(210, 231)$.

■ Corrigé de l'exercice 12

- a) Les diviseurs positifs de $2^a 3^b$ sont les $2^i 3^j$ avec $0 \leq i \leq a$ et $0 \leq j \leq b$: il y en a $(a+1)(b+1)$.

b) $36 = 2^2 \times 3^2 \mid N \iff (a \geq 2 \text{ et } b \geq 2)$. On cherche $(a+1)(b+1) = 15$ avec $a+1 \geq 3$ et $b+1 \geq 3$: $15 = 3 \times 5 = 5 \times 3$, donc $(a, b) \in \{(2, 4), (4, 2)\}$: $N = 2^2 \times 3^4 = 324$ ou $N = 2^4 \times 3^2 = 144$.

c) $324 = 18^2$ et $144 = 12^2$. **C'était prévisible** : un entier a un nombre impair de diviseurs si et seulement si c'est un carré parfait (cours) ; ici 15 est impair.
- a) $(n^2 + 1 + n)(n^2 + 1 - n) = (n^2 + 1)^2 - n^2 = n^4 + 2n^2 + 1 - n^2 = n^4 + n^2 + 1$.

b) Pour $n \in \mathbb{N}$: $1 \leq n^2 - n + 1 \leq n^2 + n + 1$ (car $n^2 - n = n(n-1) \geq 0$). Si $n^4 + n^2 + 1$ est premier, ses seuls diviseurs positifs sont 1 et lui-même : le plus petit facteur vaut 1, donc $n(n-1) = 0$, $n \in \{0, 1\}$. Or $n = 0$ donne 1 (non premier) et $n = 1$ donne 3 (premier). $n = 1$.
- a) **Raisonnons sur le reste de p par 3**. Si $p \neq 3$, p premier n'est pas multiple de 3, donc $p \equiv 1$ ou $-1 [3]$, $p^2 \equiv 1 [3]$ et $8p^2 + 1 \equiv 9 \equiv 0 [3]$.

b) Si $p \neq 3$: $3 \mid 8p^2 + 1$ et $8p^2 + 1 \geq 33 > 3$, donc $8p^2 + 1$ n'est pas premier. Si $p = 3$: $8p^2 + 1 = 73$, premier ($8^2 < 73 < 9^2$, ni 2, ni 3, ni 5, ni 7 ne le divisent). $p = 3$.

■ Corrigé de l'exercice 13

- $7 \times 11 \times 13 = 77 \times 13 = 1001$. Donc $1000 = 1001 - 1 \equiv -1 [1001]$, et cette congruence reste vraie modulo chaque diviseur 7, 11, 13 de 1001.
- Compatibilité avec les puissances** : $1000^i \equiv (-1)^i [1001]$, d'où $N = \sum t_i 1000^i \equiv \sum (-1)^i t_i [1001]$, puis modulo 7, 11 et 13. **Critère** : N et la somme alternée de ses tranches $t_0 - t_1 + t_2 - \dots$ ont le même reste par 7 (par 11, par 13) ; en particulier N est divisible par 7 (resp. 11, 13) si et seulement si cette somme l'est.
- a) Tranches : $t_0 = 828$, $t_1 = 281$, $t_2 = 718$, $t_3 = 2$; $828 - 281 + 718 - 2 = 1263 = 7 \times 180 + 3 = 11 \times 114 + 9 = 13 \times 97 + 2$. Restes : 3 par 7, 9 par 11, 2 par 13.

b) $\overline{abcabc} = 1000 \times \overline{abc} + \overline{abc} = 1001 \times \overline{abc}$: divisible par 7, 11 et 13.
- Double implication**. Si $7 \mid N$, alors $7 \mid 21a - 2N = 21a - 20a - 2u = a - 2u$. Réciproquement, si $7 \mid a - 2u$, alors $7 \mid 10(a - 2u) + 21u = 10a + u = N$. $3157 : a - 2u = 315 - 14 = 301 = 7 \times 43$: $7 \mid 3157$ ($3157 = 7 \times 451$).

■ Corrigé de l'exercice 14

1. $(x-3)(y-2) = xy - 2x - 3y + 6$: l'équation équivaut à $(x-3)(y-2) = 6$. $x-3$ est un diviseur de 6 et $y-2 = \frac{6}{x-3}$:

$x-3$	1	2	3	6	-1	-2	-3	-6
$y-2$	6	3	2	1	-6	-3	-2	-1
(x, y)	(4, 8)	(5, 5)	(6, 4)	(9, 3)	(2, -4)	(1, -1)	(0, 0)	(-3, 1)

8 solutions, celles du tableau.

2. $x^2 - y^2 = (x-y)(x+y) = 45$. **Signes et parités** : $x+y \geq 0$ et le produit est positif, donc $0 < x-y \leq x+y$; et $x-y, x+y$ ont même parité (leur somme $2x$ est paire). $(x-y, x+y) \in \{(1, 45), (3, 15), (5, 9)\}$, d'où $(x, y) \in \{(23, 22), (9, 6), (7, 2)\}$. Dans $\mathbb{Z}^2$: (x, y) est solution si et seulement si $(|x|, |y|)$ l'est, et chaque solution de $\mathbb{N}^2$ (avec $x, y \neq 0$) donne 4 choix de signes : **12** solutions.
3. a) r^2 modulo 5 vaut 0, 1, 4, 4, 1 pour $r = 0, \dots, 4$: restes possibles **0, 1, 4**. b) **Par l'absurde** : une solution donnerait $x^2 \equiv x^2 - 5y^2 = 2027 \equiv 2 \pmod{5}$, ce qui est impossible d'après a). **Pas de solution.**

■ Corrigé de l'exercice 15

1. **On teste tous les restes r modulo n .** a) $5r$ modulo 8 : 0, 5, 2, 7, 4, 1, 6, 3 ($r = 0, \dots, 7$) : **$x \equiv 7 \pmod{8}$** . b) $6r$ modulo 15 ($r = 0, \dots, 14$) : 0, 6, 12, 3, 9, répétés trois fois ; 9 est obtenu pour $r \in \{4, 9, 14\}$: **$x \equiv 4 \pmod{5}$** . c) $4x - 7$ est impair, il n'est jamais multiple de 10 : **aucune solution**.
2. a) $r^2 + r + 1$ pour $r = 0, \dots, 6$: 1, 3, 7, 13, 21, 31, 43, de restes 1, 3, 0, 6, 0, 3, 1 par 7 : **$x \equiv 2$ ou $4 \pmod{7}$** . b) $x^2 \equiv x \iff x(x-1) \equiv 0 \pmod{12}$; $r(r-1)$ modulo 12 pour $r = 0, \dots, 11$: 0, 0, 2, 6, 0, 8, 6, 6, 8, 0, 6, 2 : **$x \equiv 0, 1, 4$ ou $9 \pmod{12}$** . **Remarque** : pour $x \equiv 4$, $x(x-1) \equiv 0 \pmod{12}$ sans que x ni $x-1$ soit $\equiv 0 \pmod{12}$: modulo 12 (non premier), un produit peut être nul sans qu'aucun facteur le soit ($4 \times 3 = 12$).
3. a) **On substitue** : $x = 3k + 2 \equiv 3 \pmod{5} \iff 3k \equiv 1 \pmod{5} \iff k \equiv 2 \pmod{5}$ ($3r$ modulo 5 : 0, 3, 1, 4, 2). Donc $k = 5j + 2$ et $x = 15j + 8$; réciproquement, $15j + 8 \equiv 2 \pmod{3}$ et $\equiv 3 \pmod{5}$. **$x \equiv 8 \pmod{15}$** . b) $100 \leq 15j + 8 \leq 120 \iff j = 7$: **113** œufs.

■ Corrigé de l'exercice 16

1. a) $n^4 - n^2 = n^2(n^2 - 1) = n \times (n-1)n(n+1)$. Parmi trois entiers consécutifs $n-1, n, n+1$, l'un est multiple de 3 : $3 \mid n^4 - n^2$. **Disjonction des cas** : si $n = 2k$, $4 \mid 4k^2 = n^2$; si n est impair, $n-1$ et $n+1$ sont pairs, donc $4 \mid n^2 - 1$. Dans les deux cas, $4 \mid n^4 - n^2$. b) $3 \mid n^4 - n^2$, $4 \mid n^4 - n^2$ et $3 \wedge 4 = 1$, donc (cours) **$12 \mid n^4 - n^2$** . **Non** pour 24 : $n = 2$ donne $16 - 4 = 12$.
2. Soit $d = (2n+3) \wedge (5n+7)$: $d \mid 5(2n+3) - 2(5n+7) = 1$, donc $d = 1$: la fraction est **irréductible**.
3. $a = 15a'$, $b = 15b'$ avec $a' \wedge b' = 1$ et $a' + b' = 8$. On écarte (0, 8) et (8, 0) ($0 \wedge 8 = 8$), (2, 6), (4, 4), (6, 2) (facteur 2) : $(a', b') \in \{(1, 7), (3, 5), (5, 3), (7, 1)\}$. **$(a, b) \in \{(15, 105), (45, 75), (75, 45), (105, 15)\}$** .

28

Corrigés du niveau 3

■ Corrigé de l'exercice 17

1. a) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$ (on développe : les termes se simplifient deux à deux), et le second facteur est entier. b) $2^{15} - 1 = 8^5 - 1^5$ est divisible par $8 - 1 = 7$, et $2^{15} - 1 = 32^3 - 1^3$ par $32 - 1 = 31$. Comme $7 \wedge 31 = 1$, $217 \mid 32\,767$, et $32\,767 = 217 \times 151$, où 151 est premier ($12^2 < 151 < 13^2$, ni 2, 3, 5, 7, 11 ne le divisent) : **$2^{15} - 1 = 7 \times 31 \times 151$** .
2. a) $2^{a-b}(2^b - 1) + 2^{a-b} - 1 = 2^a - 2^{a-b} + 2^{a-b} - 1 = 2^a - 1$. b) **Lemme du cours** : si $A = BQ + R$, les diviseurs communs de A et B sont ceux de B et R , donc $A \wedge B = B \wedge R$. Avec $A = 2^a - 1$, $B = 2^b - 1$, $Q = 2^{a-b}$, $R = 2^{a-b} - 1$: c'est l'égalité demandée. c) **Récurrence forte sur $s = a + b \geq 2$** . **Initialisation** : $s = 2$, $a = b = 1$: $1 \wedge 1 = 1 = 2^1 - 1$. **Hérédité** : soit $s \geq 3$; supposons la formule vraie pour tous $a, b \geq 1$ de somme $< s$, et soit $a + b = s$, avec par exemple $a \geq b$. Si $a = b$: $(2^a - 1) \wedge (2^a - 1) = 2^a - 1 = 2^{a \wedge a} - 1$. Si $a > b$: par b), $(2^a - 1) \wedge (2^b - 1) = (2^{a-b} - 1) \wedge (2^b - 1)$, avec $a-b \geq 1$ et $(a-b) + b = a < s$: c'est $2^{(a-b) \wedge b} - 1 = 2^{a \wedge b} - 1$, car $(a-b) \wedge b = a \wedge b$. **Conclusion** : **$(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$** pour tous $a, b \in \mathbb{N}^*$.

3. $84 \wedge 60 = 12 : (2^{84} - 1) \wedge (2^{60} - 1) = 2^{12} - 1 = \boxed{4095}$. $2026 \wedge 2025 = 1$ (consécutifs) : le PGCD vaut $2^1 - 1 = 1$: **premiers entre eux**.

■ Corrigé de l'exercice 18

1. **Disjonction des cas selon le reste de x par 3.** $(3k)^3 = 27k^3 \equiv 0$; $(3k+1)^3 = 27k^3 + 27k^2 + 9k + 1 \equiv 1$; $(3k-1)^3 = 27k^3 - 27k^2 + 9k - 1 \equiv -1$ [9].
2. Chaque cube est congru à $-1, 0$ ou 1 modulo 9, donc une somme de trois cubes est congrue à un entier de $\{-3, \dots, 3\}$, c'est-à-dire à $6, 7, 8, 0, 1, 2$ ou 3 modulo 9 : **jamais à 4 ni à 5**. 2030 a pour somme des chiffres 5 : $2030 \equiv 5$ [9], **ce n'est pas** une somme de trois cubes.
3. **Contraposée** : si aucun des entiers x, y, z n'est multiple de 3, leurs cubes sont $\equiv \pm 1$ [9], et leur somme est $\equiv -3, -1, 1$ ou 3 [9] : jamais 0. Donc $9 \mid x^3 + y^3 + z^3 \Rightarrow \boxed{3 \mid xyz}$.
4. **Avec 1.** : parmi $1, \dots, 100$, il y a 34 entiers $\equiv 1$ [3] ($1, 4, \dots, 100$), 33 entiers $\equiv -1$ [3] et 33 multiples de 3 : $S \equiv 34 - 33 = 1$ [9]. **Avec la formule** : $S = 5050^2$ et $5050 \equiv 5 + 0 + 5 + 0 = 10 \equiv 1$ [9], donc $S \equiv 1$. Reste $\boxed{1}$.

■ Corrigé de l'exercice 19

1. a) $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ et $x^2 + xy + y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 \geq 0$, nul seulement si $x = y = 0$ (exclu car $91 \neq 0$). Le produit valant $91 > 0$, $x - y > 0$, et $d = x - y$ est un diviseur positif de 91 : $d \in \{1, 7, 13, 91\}$.
b) $3(x + y)^2 + (x - y)^2 = 4x^2 + 4xy + 4y^2$ ✓. Avec $s = x + y$: $3s^2 + d^2 = \frac{4 \times 91}{d}$, donc **(encadrement)** $d^2 \leq \frac{364}{d}$, $d^3 \leq 364$, et $d \in \{1, 7\}$ ($13^3 > 364$). $d = 1$: $3s^2 = 363$, $s = \pm 11$; $d = 7$: $3s^2 = 3$, $s = \pm 1$. Avec $x = \frac{s+d}{2}$, $y = \frac{s-d}{2}$: $(x, y) \in \{(6, 5), (-5, -6), (4, -3), (3, -4)\}$ (contrôle : $64 + 27 = 91$).
2. **Par symétrie, on suppose** $x \leq y \leq z$: $xyz = 2(x + y + z) \leq 6z$, d'où $\boxed{xy \leq 6}$, donc $x^2 \leq 6$ et $x \in \{1, 2\}$. Si $x = 1$: $yz = 2 + 2y + 2z \iff (y - 2)(z - 2) = 6$; $y = 1$ donnerait $z = -4$, et $y = 2$ donnerait $0 = 6$; donc $1 \leq y - 2 \leq z - 2$: $(y, z) \in \{(3, 8), (4, 5)\}$. Si $x = 2$: $2yz = 2(2 + y + z) \iff (y - 1)(z - 1) = 3$ avec $1 \leq y - 1 \leq z - 1$: $(y, z) = (2, 4)$. Les solutions sont les permutations de $\boxed{(1, 3, 8), (1, 4, 5), (2, 2, 4)}$: $6 + 6 + 3 = 15$ triplets.

■ Corrigé de l'exercice 20

1. a) Les diviseurs positifs de p^α sont $1, p, \dots, p^\alpha$: $\sigma(p^\alpha) = 1 + p + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$.
b) Par la formule du cours : $\sigma(2^a 3^b) = (2^{a+1} - 1) \frac{3^{b+1} - 1}{2}$.
c) $1240 = 2^3 \times 5 \times 31$, et $2^{a+1} - 1$ est un diviseur **impair** de 1240 : $2^{a+1} - 1 \in \{1, 5, 31, 155\}$; seuls 1 ($a = 0$) et 31 ($a = 4$) sont de la forme $2^k - 1$. Si $a = 0$: $3^{b+1} = 2481$, qui n'est pas une puissance de 3 ($3^7 = 2187$, $3^8 = 6561$). Si $a = 4$: $\frac{3^{b+1} - 1}{2} = 40$, $3^{b+1} = 81$, $b = 3$. $\boxed{n = 2^4 \times 3^3 = 432}$.
2. a) $\sigma(p^\alpha)$ est une somme de $\alpha + 1$ entiers impairs : elle a la parité de $\alpha + 1$, **impaire si et seulement si α est pair**.
b) Écrivons $n = 2^a p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (p_i premiers impairs). $\sigma(n) = (2^{a+1} - 1) \sigma(p_1^{\alpha_1}) \dots \sigma(p_k^{\alpha_k})$, où $2^{a+1} - 1$ est impair : $\sigma(n)$ est impair $\iff$ tous les $\sigma(p_i^{\alpha_i})$ le sont $\iff$ tous les α_i sont pairs $\iff n = 2^a m^2$ avec m impair. Si a est pair, $n = (2^{a/2} m)^2$; si a est impair, $n = 2(2^{(a-1)/2} m)^2$. Réciproquement, dans un carré ou le double d'un carré, les exposants des premiers impairs sont pairs.
 $\sigma(n)$ impair $\iff n = c^2$ ou $n = 2c^2$.
c) $\sigma(18) = \sigma(2)\sigma(3^2) = 3 \times 13 = 39$, impair : $18 = 2 \times 3^2$ ✓. $\sigma(12) = \sigma(2^2)\sigma(3) = 7 \times 4 = 28$, pair : 12 n'est ni un carré, ni le double d'un carré ✓.

■ Corrigé de l'exercice 21

Outil : $a = da'$, $b = db'$ avec $a' \wedge b' = 1$, et $m = da'b'$, donc $dm = ab$ (cours).

- $576(a'^2 + b'^2) = 7488$, soit $a'^2 + b'^2 = 13$. Les carrés ≤ 13 sont 0, 1, 4, 9 : $\{a', b'\} = \{2, 3\}$ (premiers entre eux ✓). $(a, b) \in \{(48, 72), (72, 48)\}$.
- $(a - d)(b - d) = ab - d(a + b) + d^2 = dm - d(d + m) + d^2 = 0$. Donc $a = d$ ou $b = d$: si $a = d$, a divise b ; si $b = d$, b divise a .
- Par l'absurde :** $m = a + b$ donne $da'b' = d(a' + b')$, soit $(a' - 1)(b' - 1) = 1$, donc $a' = b' = 2$ ($a', b' \geq 1$) ; mais alors $a' \wedge b' = 2 \neq 1$: **contradiction**.
- $m = a + b + 3d \iff a'b' = a' + b' + 3 \iff (a' - 1)(b' - 1) = 4$, avec $a' - 1, b' - 1 \geq 0$: $(a', b') \in \{(2, 5), (3, 3), (5, 2)\}$, et $(3, 3)$ est exclu ($3 \wedge 3 = 3$). Réciproquement, $2d \vee 5d = 10d = 2d + 5d + 3d$ ✓. $(a, b) = (2d, 5d)$ ou $(5d, 2d)$, $d \in \mathbb{N}^*$.

■ Corrigé de l'exercice 22

- Encadrement :** pour $n \geq 1$, $n^2 < n^2 + n < n^2 + 2n + 1$, soit $n^2 < n(n + 1) < (n + 1)^2$. Il n'y a aucun carré strictement entre deux carrés consécutifs : $n(n + 1)$ n'est pas un carré.
- a) Avec $t = n^2 + 3n$: $n(n + 3) = t$ et $(n + 1)(n + 2) = t + 2$, donc $n(n + 1)(n + 2)(n + 3) + 1 = t(t + 2) + 1 = (t + 1)^2 = (n^2 + 3n + 1)^2$.
b) Pour $n \geq 1$: $P = n(n + 1)(n + 2)(n + 3) = (t + 1)^2 - 1$ vérifie $t^2 < t^2 + 2t = P < (t + 1)^2$ ($t > 0$) : P n'est pas un carré. c) $2023^2 + 3 \times 2023 + 1 = 4\,092\,529 + 6069 + 1$: la racine vaut $\boxed{4\,098\,599}$.
- a) **Par la décomposition :** a et b n'ont aucun facteur premier commun, donc la décomposition de ab s'obtient en juxtaposant celles de a et de b , avec les mêmes exposants. ab étant un carré, tous ces exposants sont pairs : a et b sont des carrés.
b) Si $d \mid n + 1$ et $d \mid n(n + 2)$, alors $d \mid (n + 1)^2 - n(n + 2) = 1$: $(n + 1) \wedge n(n + 2) = 1$. **Par l'absurde**, si $n(n + 1)(n + 2)$ ($n \geq 1$) était un carré, $n + 1$ et $n(n + 2)$ seraient des carrés (par a) ; or $n^2 < n^2 + 2n = n(n + 2) < (n + 1)^2$: **contradiction**.

■ Corrigé de l'exercice 23

Rappel : un carré est $\equiv 0$ ou $1 \pmod{4}$.

- Si $x \geq 2$, $2^x - 1 \equiv -1 \equiv 3 \pmod{4}$: pas un carré. $x = 0$: $y^2 = 0$; $x = 1$: $y^2 = 1$. $\boxed{(0, 0), (1, 1)}$. b) Si $x \geq 2$, $2^x + 3 \equiv 3 \pmod{4}$: impossible ; $x = 0$: $y^2 = 4$; $x = 1$: $y^2 = 5$, impossible. $\boxed{(0, 2)}$.
- $(y - 1)(y + 1) = 2^x$, avec $y \geq 2$ ($y = 0, 1$ donnent $-1, 0$). **Les seuls diviseurs positifs de 2^x sont des puissances de 2 :** $y - 1 = 2^\alpha$, $y + 1 = 2^\beta$, $\beta > \alpha$, et $2^\alpha(2^{\beta-\alpha} - 1) = 2$. Le facteur $2^{\beta-\alpha} - 1$ est impair : il vaut 1, et $2^\alpha = 2$: $\alpha = 1$, $\beta = 2$, $y = 3$, $x = 3$. $\boxed{(3, 3)}$.
- De même $(y - 1)(y + 1) = 3^x$, $y \geq 2$: $y - 1 = 3^\alpha$, $y + 1 = 3^\beta$ avec $3^\beta - 3^\alpha = 2$; si $\alpha \geq 1$, $3 \mid 2$: absurde. Donc $\alpha = 0$, $y = 2$, $3^x = 3$. $\boxed{(1, 2)}$.
- $(y - 1)(y^2 + y + 1) = 2^x$. Or $y^2 + y + 1 = y(y + 1) + 1$ est **impair** et divise 2^x : il vaut 1, donc $y = 0$, et alors $2^x = -1$: absurde. $\boxed{\text{Aucune solution}}$.

29

Corrigés du niveau 4

■ Corrigé de l'exercice 24

- a) $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1)$.
b) **Disjonction des cas modulo 5.** Si $n \equiv 0, 1$ ou $-1 \pmod{5}$, l'un des facteurs $n, n - 1, n + 1$ est multiple de 5. Si $n \equiv \pm 2 \pmod{5}$, $n^2 + 1 \equiv 5 \equiv 0 \pmod{5}$. Donc $5 \mid n^5 - n$. De plus $6 \mid (n - 1)n(n + 1)$ (trois consécutifs, cours). Comme $6 \wedge 5 = 1$: $\boxed{30 \mid n^5 - n}$.

- c) Si n est impair : $8 \mid n^2 - 1$ (un carré impair est $\equiv 1 [8]$) et $n^2 + 1$ est pair, donc $16 \mid (n^2 - 1)(n^2 + 1)$. Avec $3 \mid n^5 - n$, $5 \mid n^5 - n$ et $16, 3, 5$ premiers entre eux deux à deux : $240 \mid n^5 - n$.
2. $10 \mid 30 \mid n^5 - n : n^5 \equiv n [10]$, même chiffre des unités ($n \in \mathbb{N}$). Puis $(a^5 + b^5 + c^5) - (a + b + c) = (a^5 - a) + (b^5 - b) + (c^5 - c) \equiv 0 [30]$: les deux sommes ont le même reste par 30, d'où l'équivalence.
3. On remplace chaque k^5 par $k : S \equiv 1 + 2 + \dots + 2026 = \frac{2026 \times 2027}{2} = 2\,053\,351 = 30 \times 68\,445 + 1 [30]$. Reste $\boxed{1}$; comme $10 \mid 30, S \equiv 1 [10]$: chiffre des unités $\boxed{1}$.
4. $a^5 b - ab^5 = b(a^5 - a) - a(b^5 - b)$ (développer : $a^5 b - ab - ab^5 + ab$) : c'est une combinaison de deux multiples de 30, donc $30 \mid a^5 b - ab^5$.

■ Corrigé de l'exercice 25

1. r^2 modulo 8 pour $r = 0, \dots, 7$: 0, 1, 4, 1, 0, 1, 4, 1 : restes $\boxed{0, 1, 4}$. Une somme de trois éléments de $\{0, 1, 4\}$ vaut 0, 1, 2, 3, 4, 5, 6, 8, 9 ou 12, de reste 0, 1, 2, 3, 4, 5 ou 6 par 8 : **jamais** 7. $2023 = 8 \times 252 + 7$ n'est donc pas somme de trois carrés.
2. a) Un carré est $\equiv 0 [4]$ si l'entier est pair, $\equiv 1 [4]$ s'il est impair. Si j des trois entiers sont impairs, $x^2 + y^2 + z^2 \equiv j [4]$, avec $0 \leq j \leq 3$: la somme est $\equiv 0 [4]$ seulement si $j = 0$: x, y, z **sont pairs**.
b) **Récurrence sur a** , avec $\mathcal{P}(a)$: « pour tout $b \in \mathbb{N}$, $4^a(8b + 7)$ n'est pas somme de trois carrés ». Initialisation : c'est 1. Hérédité : si $4^{a+1}(8b + 7) = x^2 + y^2 + z^2$, cette somme est $\equiv 0 [4]$, donc x, y, z sont pairs (a) et $4^a(8b + 7) = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2$, ce qui contredit $\mathcal{P}(a)$. Conclusion : $\mathcal{P}(a)$ est vraie pour tout a . Exemples : $60 = 4 \times (8 + 7)$, $112 = 4^2 \times 7$.
3. a) Le second membre est pair ($k \geq 1$), donc $x^2 + y^2 + z^2$ aussi : 0 ou 2 des entiers sont impairs. S'il y en a 2, l'autre est pair, $x^2 + y^2 + z^2 \equiv 1 + 1 + 0 = 2 [4]$, tandis que $2^k xyz$ est divisible par 2^{k+1} , donc par 4 : **contradiction**. Donc $x = 2x', y = 2y', z = 2z'$, et $4(x'^2 + y'^2 + z'^2) = 2^k \times 8x'y'z'$, soit $x'^2 + y'^2 + z'^2 = 2^{k+1}x'y'z' : (x', y', z')$ est solution de (E_{k+1}) .
b) **Descente infinie**. Soit (x, y, z) une solution de (E_1) . Par récurrence sur j , avec a) : $\left(\frac{x}{2^j}, \frac{y}{2^j}, \frac{z}{2^j}\right)$ est une solution entière de (E_{1+j}) pour tout $j \in \mathbb{N}$. Donc $2^j \mid x$ pour tout j : si $x \neq 0$, on aurait $2^j \leq |x|$ pour tout j , ce qui est faux. Ainsi $x = 0$, de même $y = z = 0$; et $(0, 0, 0)$ convient. $S = \{(0, 0, 0)\}$.

■ Corrigé de l'exercice 26

1. $D = \left(n + \frac{1}{2}\right)^2 + \frac{3}{4} > 0$ et D est entier : $D \geq 1$. $n^3 - 1 = (n - 1)(n^2 + n + 1)$, donc $D \mid n^3 - 1 : \boxed{n^3 \equiv 1 [D]}$.
2. **On réduit l'exposant modulo 3**. Soit $k = 3q + r$ ($r \in \{0, 1, 2\}$) : $n^k = (n^3)^q n^r \equiv n^r$ et $n^{2k} = (n^3)^{2q} n^{2r} \equiv n^{2r} [D]$. Si $r = 1$: $n^{2k} + n^k + 1 \equiv n^2 + n + 1 = D \equiv 0$. Si $r = 2$: $n^{2k} + n^k + 1 \equiv n^4 + n^2 + 1 = n^3 \times n + n^2 + 1 \equiv n + n^2 + 1 \equiv 0 [D]$. Si $r = 0$: $n^{2k} + n^k + 1 \equiv 3 [D]$, donc $D \mid n^{2k} + n^k + 1 \iff D \mid 3 \iff D \in \{1, 3\}$: $n^2 + n = 0$ ou $n^2 + n - 2 = (n - 1)(n + 2) = 0$, soit $\boxed{n \in \{-2, -1, 0, 1\}}$.
3. a) $k = 1013 = 3 \times 337 + 2$ n'est pas multiple de 3 : $n^2 + n + 1 \mid n^{2026} + n^{1013} + 1$ pour tout n . b) Avec $n = 2$: $D = 7$ divise $4^k + 2^k + 1$ si $3 \nmid k$; pour $k \geq 2$, $4^k + 2^k + 1 \geq 21 > 7$: **composé** (exemple : $4^2 + 2^2 + 1 = 21 = 3 \times 7$).

4. $n^4 = n^3 \times n \equiv n [D]$, donc $n^4 + 3n + 5 \equiv 4n + 5 [D]$, et $D \mid n^4 + 3n + 5 \iff D \mid 4n + 5$. Comme $4n + 5 \neq 0$ (impair), il faut $D \leq |4n + 5|$. Si $n \geq 0$: $n^2 + n + 1 \leq 4n + 5 \iff (n - 4)(n + 1) \leq 0 \iff n \leq 4$. Si $n \leq -2$: $n^2 + n + 1 \leq -4n - 5 \iff (n + 2)(n + 3) \leq 0 \iff n \in \{-3, -2\}$. Avec $n = -1$, il reste à tester $n \in \{-3, \dots, 4\}$:

n	-3	-2	-1	0	1	2	3	4
D	7	3	1	1	3	7	13	21
$4n + 5$	-7	-3	1	5	9	13	17	21
$D \mid 4n + 5$?	oui	oui	oui	oui	oui	non	non	oui

$n \in \{-3, -2, -1, 0, 1, 4\}$ (contrôle : $n = 4$, $273 = 21 \times 13$).

■ Corrigé de l'exercice 27

- $2^{10} = 1024 \leq 2026 < 2^{11}$: $v(2026!) = 1013 + 506 + 253 + 126 + 63 + 31 + 15 + 7 + 3 + 1 = \boxed{2018}$.
- a) $\frac{n}{2^k} = (a_r 2^{r-k} + \dots + a_k) + \frac{a_{k-1} 2^{k-1} + \dots + a_0}{2^k}$, et $0 \leq a_{k-1} 2^{k-1} + \dots + a_0 \leq 2^{k-1} + \dots + 1 = 2^k - 1 < 2^k$: la fraction est dans $[0, 1[$, donc $E\left(\frac{n}{2^k}\right) = a_r 2^{r-k} + \dots + a_{k+1} 2 + a_k$.
b) On somme et on regroupe selon les a_i : $v(n!) = \sum_{k=1}^r \sum_{i=k}^r a_i 2^{i-k} = \sum_{i=1}^r a_i (2^{i-1} + \dots + 2 + 1) = \sum_{i=1}^r a_i (2^i - 1) = \sum_{i=0}^r a_i 2^i - \sum_{i=0}^r a_i$ (le terme $i = 0$ est nul) : $\boxed{v(n!) = n - s(n)}$.
- a) $2026 = 1024 + 512 + 256 + 128 + 64 + 32 + 8 + 2 = (11111101010)_2$: $s = 8$ et $v(2026!) = 2026 - 8 = 2018$ ✓. b) $s(n) \geq 1$, donc $v(n!) \leq n - 1 < n$: $2^n \nmid n!$. c) $2^{n-1} \mid n! \iff n - s(n) \geq n - 1 \iff s(n) = 1 \iff \boxed{n \text{ est une puissance de } 2}$.

■ Corrigé de l'exercice 28

- Pour $x, y \neq 0$, on multiplie par $nxy \neq 0$: $(E) \iff ny + nx = xy \iff xy - nx - ny + n^2 = n^2 \iff \boxed{(x - n)(y - n) = n^2}$.
- a) Si $x, y > 0$: $\frac{1}{x} < \frac{1}{x} + \frac{1}{y} = \frac{1}{n}$, donc $x > n$; de même $y > n$. b) **Bijection avec les diviseurs** : si $(x, y) \in (\mathbb{N}^*)^2$ est solution, $u = x - n$ est un diviseur positif de n^2 et $y = n + \frac{n^2}{u}$. Réciproquement, tout diviseur $u > 0$ de n^2 donne la solution $(n + u, n + \frac{n^2}{u}) \in (\mathbb{N}^*)^2$. Deux diviseurs distincts donnent deux solutions distinctes : $\boxed{d(n^2) \text{ solutions}}$.
- Dans $(\mathbb{Z}^*)^2$, $u = x - n$ décrit les diviseurs de n^2 , positifs ou négatifs, à condition que $x = n + u \neq 0$ et $y = n + \frac{n^2}{u} \neq 0$. Pour $u > 0$, aucun problème : $d(n^2)$ solutions. Pour $u < 0$: $x = 0 \iff u = -n \iff y = 0$; il faut exclure le seul diviseur $u = -n$: $d(n^2) - 1$ solutions. Total : $\boxed{2d(n^2) - 1}$.
- a) $n^2 = 100$; $x \leq y$ impose $u \leq 10$, soit $u \in \{1, 2, 4, 5, 10\}$: les solutions sont $\boxed{(11, 110), (12, 60), (14, 35), (15, 30), (20, 20)}$. b) $60^2 = 2^4 \times 3^2 \times 5^2$: $d = 5 \times 3 \times 3 = 45$: $\boxed{45}$ solutions dans $(\mathbb{N}^*)^2$ et $\boxed{89}$ dans $(\mathbb{Z}^*)^2$. $2026 = 2 \times 1013$ (1013 est premier : aucun premier ≤ 31 ne le divise) : $d(2^2 \times 1013^2) = 9$: $\boxed{9}$ et $\boxed{17}$ solutions.

■ Corrigé de l'exercice 29

- Si $2^k m \leq n$ avec $m \geq 1$, alors $2^k m < 2^{k+1}$, donc $m < 2$ et $m = 1$: 2^k est le seul multiple de 2^k dans $\{1, \dots, n\}$.
- Soit $j \neq 2^k$ dans $\{1, \dots, n\}$, écrit $j = 2^v o$ avec o impair. Comme $2^v \leq j < 2^{k+1}$, $v \leq k$, et $v = k$ ferait de j un multiple de 2^k , donc $j = 2^k$ (1.) : ainsi $v \leq k - 1$. De plus o est un entier impair $\leq n$, donc un facteur de M . Ainsi $\frac{P}{j} = 2^{k-1-v} \times \frac{M}{o}$ est un entier. Mais $\frac{P}{2^k} = \frac{M}{2}$, avec M impair : **ce n'est pas un entier**.
- $PH_n = \sum_{j=1}^n \frac{P}{j} = E + \frac{M}{2}$, où $E = \sum_{j \neq 2^k} \frac{P}{j}$ est entier. **Par l'absurde** : si H_n était entier, $\frac{M}{2} = PH_n - E$ serait entier : contradiction. $\boxed{H_n \notin \mathbb{N}}$.

4. **Même méthode avec les puissances de 3.** Soit $k \geq 1$ tel que $3^k \leq 2n+1 < 3^{k+1}$. Un multiple impair de 3^k s'écrit $3^k m$ avec m impair ; si $m \geq 3$, il dépasse $2n+1$: **3^k est le seul multiple impair de 3^k dans $\{1, 3, \dots, 2n+1\}$.** Soit M' le produit des entiers impairs $\leq 2n+1$ non multiples de 3, et $Q = 3^{k-1} M'$. Pour j impair $\leq 2n+1$, $j \neq 3^k$: $j = 3^w o$ avec $3 \nmid o$, $w \leq k-1$, et o facteur de M' , donc $\frac{Q}{j}$ est entier ; et $\frac{Q}{3^k} = \frac{M'}{3}$ ne l'est pas ($3 \nmid M'$). La somme T vérifie $QT = (\text{entier}) + \frac{M'}{3}$: T n'est pas entier.

■ Corrigé de l'exercice 30

- $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$, tous premiers (257 : exercice 5). $F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = (F_n - 2)F_n$.
- Récurrence.** Soit $\mathcal{P}(n)$: « $F_0 F_1 \cdots F_{n-1} = F_n - 2$ ». *Initialisation* : $F_0 = 3 = 5 - 2 = F_1 - 2$. *Hérédité* : supposons $\mathcal{P}(n)$ vraie pour un $n \geq 1$; alors $F_0 \cdots F_{n-1} F_n = (F_n - 2)F_n = F_{n+1} - 2$ (question 1) : $\mathcal{P}(n+1)$ est vraie. *Conclusion* : $F_0 F_1 \cdots F_{n-1} = F_n - 2$ pour tout $n \geq 1$.
- a) Soit $m < n$ et $d = F_m \wedge F_n$. d divise F_m , donc le produit $F_0 \cdots F_{n-1} = F_n - 2$; il divise aussi F_n , donc $F_n - (F_n - 2) = 2 : d \in \{1, 2\}$. Or F_n est impair : $F_m \wedge F_n = 1$.
b) Chaque $F_n \geq 3$ admet un diviseur premier p_n (cours). Si $m \neq n$, alors $p_m \neq p_n$: sinon ce nombre premier diviserait $F_m \wedge F_n = 1$. Les p_n ($n \in \mathbb{N}$) sont donc des nombres premiers deux à deux distincts : **il y a une infinité de nombres premiers.**
- a) $5 \times 128 + 1 = 641$ et $625 + 16 = 641$ ✓. b) $5 \times 2^7 = 640 = 641 - 1 \equiv -1 \pmod{641}$; en élevant à la puissance 4 (compatibilité) : $5^4 \times 2^{28} \equiv (-1)^4 = 1 \pmod{641}$. c) $5^4 = 641 - 2^4 \equiv -2^4 \pmod{641}$, donc $-2^4 \times 2^{28} \equiv 1$, soit $-2^{32} \equiv 1$ et $2^{32} \equiv -1 \pmod{641}$: $641 \mid 2^{32} + 1 = F_5$. (En effet $F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$: *Fermat s'était trompé.*)
- a) **Contraposée.** Si m n'est pas une puissance de 2, il s'écrit $m = qk$ avec $q = 2^j$ et $k \geq 3$ impair. Avec $a = 2^q \geq 2$: $2^m + 1 = a^k + 1$, et $a+1 \mid a^k + 1$ (k impair, astuce du cours $a+b \mid a^k + b^k$). Comme $1 < a+1 < a^k + 1$, l'entier $2^m + 1$ **n'est pas premier**. b) Pour $n \geq 2$: $2^{2^n} = 16^{2^{n-2}}$, avec $16 \equiv 6 \pmod{10}$ et $6^j \equiv 6 \pmod{10}$ ($j \geq 1$, car $6 \times 6 = 36$) : $2^{2^n} \equiv 6$ et $F_n \equiv 7 \pmod{10}$.

30

Corrigés : divisibilité et restes

■ Corrigé de l'exercice 31

- $48 = 2^4 \times 3$ a pour diviseurs positifs 1, 2, 3, 4, 6, 8, 12, 16, 24, 48, et $D(-48) = D(48)$ contient aussi leurs opposés :

$$D(-48) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 16, \pm 24, \pm 48\} \quad (20 \text{ éléments}).$$

Puis 0 ne divise que 0, donc $x^2 - 1 \neq 0$; et $x^2 - 1 \geq -1$. Si $x^2 - 1 = -1$, alors $x = 0$, qui convient. Sinon $x^2 - 1$ est un diviseur positif de 48, et $x^2 \in \{2, 3, 4, 5, 7, 9, 13, 17, 25, 49\}$: seuls 4, 9, 25, 49 sont des carrés. $x \in \{0, \pm 2, \pm 3, \pm 5, \pm 7\}$.

- a) **Vrai** : $b = ka$ donne $b^2 = k^2 a^2$. b) **Faux** : $4 \mid 2^2$ mais $4 \nmid 2$.
c) **Vrai** : $c = (b+c) - b$ est une combinaison de deux multiples de a . d) **Faux** : $3 \mid 1+2$, mais $3 \nmid 1$ et $3 \nmid 2$.
e) **Vrai** : $b = ka$ et $c = la$ donnent $bc = (kl) a^2$.

3. Disjonction des cas. Si n est pair, $n(n+1)$ l'est ; si n est impair, $n+1$ est pair. Donc $n(n+1) = 2k$ avec $k \in \mathbb{Z}$, et

$$n(n+1)(n^2+n+2) = 2k(2k+2) = 4k(k+1).$$

D'après ce qui précède (appliqué à k), $k(k+1) = 2m$ est pair : le produit vaut $8m$. **Pour tout** $n \in \mathbb{Z}$, $8 \mid n(n+1)(n^2+n+2)$.

■ Corrigé de l'exercice 32

1. a) Les restes doivent être dans $\{0, 1, 2, 3, 4\}$:

$$-17 = 5 \times (-4) + 3,$$

$$-2 = 5 \times (-1) + 3,$$

$$18 = 5 \times 3 + 3.$$

b) Ce sont les entiers $5q + 3$ avec $q \in \mathbb{Z}$ (points espacés de 5 sur la droite). Et $-100 \leq 5q + 3 \leq 100 \iff -20,6 \leq q \leq 19,4 \iff -20 \leq q \leq 19$: 40 entiers (de -97 à 98).

2. On écrit $a = 6q + r$ avec $0 \leq r \leq 5$. Si $q = r$: $a = 7r$; réciproquement, $7r = 6r + r$ avec $0 \leq r < 6$ est la division euclidienne de $7r$ par 6 (unicité). $a \in \{0, 7, 14, 21, 28, 35\}$.

Si $q = -r$: $a = -6r + r = -5r$, et de même $a \in \{0, -5, -10, -15, -20, -25\}$ (par exemple $-25 = 6 \times (-5) + 5$).

3. $(n+1)(-n) + n = -n^2 - n + n = -n^2$ et $0 \leq n < n+1$: par unicité, $-n^2 = (n+1) \times (-n) + n$ (quotient $-n$, reste n).

Pour $n \geq 1$: $n(-n-1) + (n-1) = -n^2 - 1$ et $0 \leq n-1 < n$: $-n^2 - 1 = n \times (-n-1) + (n-1)$.

Avec $n = 45$ ($45^2 = 2025$) : $-2025 = 46 \times (-45) + 45$ et $-2026 = 45 \times (-46) + 44$.

■ Corrigé de l'exercice 33

On raisonne par *analyse* (une combinaison qui élimine n donne des candidats) puis *synthèse* (on teste chaque candidat).

1. a) Si $2n-1 \mid 3n+4$, il divise $2(3n+4) - 3(2n-1) = 11$: $2n-1 \in \{-11, -1, 1, 11\}$, soit $n \in \{-5, 0, 1, 6\}$. Synthèse : $-11 \mid -11, -1 \mid 4, 1 \mid 7, 11 \mid 22$. $S = \{-5, 0, 1, 6\}$.

b) Si $3n+3 \mid 2n+5$, il divise $3(2n+5) - 2(3n+3) = 9$; comme $3 \mid 3n+3$: $3n+3 \in \{-9, -3, 3, 9\}$, soit $n \in \{-4, -2, 0, 2\}$. Synthèse : $-9 \nmid -3, -3 \nmid 1, 3 \nmid 5$, mais $9 \mid 9$. $S = \{2\}$. La condition « $3n+3 \mid 9$ » n'était que nécessaire : on a multiplié $2n+5$ par 3, facteur commun avec $3n+3$.

c) $4(n^2+4) - (2n+1)(2n-1) = 4n^2 + 16 - (4n^2 - 1) = 17$: si $2n+1 \mid n^2+4$, il divise cette combinaison, donc $2n+1 \in \{\pm 1, \pm 17\}$ et $n \in \{-9, -1, 0, 8\}$. Synthèse : $-17 \mid 85, -1 \mid 5, 1 \mid 4, 17 \mid 68$. $S = \{-9, -1, 0, 8\}$.

2. a) $n^2 + 2n + 9 = (n^2 + 3) + 2(n+3)$: si $n^2 + 3$ divise l'un des entiers $n^2 + 2n + 9$ et $2(n+3)$, il divise l'autre (différence ou somme avec $n^2 + 3$).

b) Si $n \neq -3$, alors $2(n+3) \neq 0$ et $n^2 + 3 \leq 2|n+3|$. Pour $n > -3$: $n^2 - 2n - 3 = (n-3)(n+1) \leq 0$, d'où $-1 \leq n \leq 3$; pour $n < -3$: $n^2 + 3 \leq -2n - 6 \iff (n+1)^2 + 8 \leq 0$, impossible.

c) Pour $n = -1, 0, 1, 2, 3$: $n^2 + 3 = 4, 3, 4, 7, 12$ et $2(n+3) = 4, 6, 8, 10, 12$: seul $n = 2$ échoue. Pour $n = -3$: $12 \mid 0$. $S = \{-3, -1, 0, 1, 3\}$.

■ Corrigé de l'exercice 34

1. Si $n = 5q + r$, alors $n^2 = 5(5q^2 + 2qr) + r^2$: n^2 a le même reste que r^2 (de même modulo 4).

reste de n par 5	0	1	2	3	4
reste de n^2 par 5	0	1	4	4	1

reste de n par 4	0	1	2	3
reste de n^2 par 4	0	1	0	1

Un carré a donc pour reste 0, 1 ou 4 par 5, et 0 ou 1 par 4.

2. $S_4 = (n^2 - 2n + 1) + n^2 + (n^2 + 2n + 1) + (n^2 + 4n + 4) = 4n^2 + 4n + 6 = 4(n^2 + n + 1) + 2$: reste 2 par 4, **jamais un carré**.

$S_6 = S_4 + (n - 2)^2 + (n + 3)^2 = S_4 + 2n^2 + 2n + 13 = 6n^2 + 6n + 19$. Avec $n(n + 1) = 2k$ (exercice 31) : $S_6 = 12k + 19 = 4(3k + 4) + 3$, reste 3 par 4 : **jamais un carré**.

3. a) Les doubles produits s'éliminent ($-4n - 2n + 2n + 4n = 0$) : $S_5 = 5n^2 + 2(1 + 4) = 5(n^2 + 2)$.

b) D'après le tableau, $n^2 + 2$ a pour reste 2, 3 ou 1 par 5 (car $4 + 2 = 6$) : $5 \nmid n^2 + 2$. Si $5 \mid m^2$, le reste de m^2 est 0, ce qui n'arrive que si $5 \mid m$; alors $m = 5k$ et $m^2 = 25k^2$.

c) Par l'absurde, si $S_5 = m^2$, alors $5 \mid m^2$, donc $25 \mid m^2 = 5(n^2 + 2)$ et $5 \mid n^2 + 2$: contradiction.

S_5 n'est jamais un carré.

4. $\sum_{k=-5}^5 (n+k)^2 = 11n^2 + 2n \sum_{k=-5}^5 k + 2(1 + 4 + 9 + 16 + 25) = 11(n^2 + 10)$. Pour $n = 23$ (entiers de 18 à 28) : $11 \times 539 = 11^2 \times 7^2$, soit $18^2 + 19^2 + \dots + 28^2 = 77^2$.

Remarque. pour deux carrés consécutifs, c'est possible : $3^2 + 4^2 = 5^2$, $20^2 + 21^2 = 29^2$.

■ Corrigé de l'exercice 35

1. $a + b \neq 0$, donc $ab \leq a + b$, soit $ab - a - b + 1 \leq 1$: $(a - 1)(b - 1) \leq 1$. Alors $a - 1$ et $b - 1$ sont des entiers naturels de produit ≤ 1 : $a = 1$, ou $b = 1$, ou $a = b = 2$. Si $a = 1$: $b \mid b + 1$, donc $b \mid (b + 1) - b = 1$ et $b = 1$; de même si $b = 1$. Enfin $4 \mid 4$. $(a, b) \in \{(1, 1), (2, 2)\}$.

2. a) $b \mid a + 1$ et $a + 1 > 0$: $a + 1 = kb$ avec $k \geq 1$. Comme $a \leq b$: $kb \leq b + 1$, soit $(k - 1)b \leq 1$. Donc $k = 1$ et $b = a + 1$, ou bien $k = 2$ et $b = 1$, et alors $a = 1$.

b) Si $b = a + 1$: $a \mid b + 1 = a + 2$, donc $a \mid 2$ et $a \in \{1, 2\}$: (1, 2) et (2, 3) conviennent ($1 \mid 3$, $2 \mid 2$; $2 \mid 4$, $3 \mid 3$). Avec (1, 1) et par symétrie :

$$(a, b) \in \{(1, 1), (1, 2), (2, 1), (2, 3), (3, 2)\}.$$

3. Supposons $a \leq b$: $a + 2 = kb$ avec $(k - 1)b \leq 2$, d'où trois cas. $k = 1$: $b = a + 2$ et $a \mid a + 4$, donc $a \mid 4$: (1, 3), (2, 4), (4, 6), qui conviennent. $k = 2$ et $b \leq 2$: $a = 2b - 2 \geq 1$ impose $b = 2$, $a = 2$. $k = 3$ et $b = 1$: $a = 1$. Par symétrie, **8 couples** :

$$(1, 1), (2, 2), (1, 3), (3, 1), (2, 4), (4, 2), (4, 6), (6, 4).$$

■ Corrigé de l'exercice 36

1. On calcule (et
- $720 = 21 \times 34 + 6$
-) :

n	1	2	3	4	5	6
T_n	1	3	6	10	15	21
$n!$	1	2	6	24	120	720
$T_n \mid n! ?$	oui	non	oui	non	oui	non

2. $n! = n(n-1)!$. Si $n! = kT_n$ ($k \in \mathbb{Z}$), alors $n(n-1)! = \frac{kn(n+1)}{2}$, soit (on divise par $n \neq 0$) $2(n-1)! = k(n+1)$; et réciproquement. $T_n \mid n! \iff n+1 \mid 2(n-1)!$.
3. Par l'absurde, si $p \mid 2 \times 1 \times 2 \times \dots \times (n-1)$, le lemme dit que p divise l'un des facteurs, tous compris entre 1 et $p-1$ (car $n-1 = p-2$ et $2 < p$); or un diviseur positif d'un entier $m \geq 1$ est $\leq m$. Contradiction : $p \nmid 2(n-1)!$, et $T_n \nmid n!$.
4. a) $b = \frac{n+1}{a} \leq \frac{n+1}{2} \leq n-1$ (car $n \geq 3$). Ainsi $2 \leq a < b \leq n-1$: a et b sont deux facteurs distincts de $1 \times 2 \times \dots \times (n-1)$, donc $(n-1)! = abm$ et $ab \mid (n-1)!$.
- b) $n+1 = a^2 \geq 5$, donc $a \geq 3$; alors $2a \leq a^2 - 2 = n-1$, car $a^2 - 2a - 2 = (a-1)^2 - 3 \geq 1$. Comme $a < 2a \leq n-1$: $(n-1)! = a \times 2a \times m$, et $a^2 \mid (n-1)!$.
- Dans les deux cas $n+1 \mid (n-1)!$, donc $n+1 \mid 2(n-1)!$ et $T_n \mid n!$.
5. Les cas $n+1 = 2$ ($n=1$) et $n+1 = 4$ ($n=3$) ont été traités en 1 (oui), les autres en 3 et 4 :

$$T_n \mid n! \iff n+1 \text{ n'est pas un nombre premier impair.}$$

Pour $1 \leq n \leq 100$, $n+1$ décrit $\{2, \dots, 101\}$, qui contient 26 nombres premiers dont 25 impairs : 75 entiers.

31 Corrigés : congruences

■ Corrigé de l'exercice 37

1. D'après le cours, $a \equiv S(a)$, $b \equiv S(b)$ et $c \equiv S(c)$ [9]. Par compatibilité avec la multiplication, si $ab = c$: $S(a) \times S(b) \equiv ab = c \equiv S(c)$ [9].
2. On calcule les restes modulo 9 (sommes des chiffres) :

calcul	$S(a)$	$S(b)$	$S(a)S(b)$ modulo 9	$S(c)$ modulo 9	conclusion
a)	$22 \equiv 4$	$18 \equiv 0$	0	$36 \equiv 0$	cohérent
b)	$13 \equiv 4$	$19 \equiv 1$	4	$21 \equiv 3$	faux
c)	$16 \equiv 7$	$19 \equiv 1$	7	$25 \equiv 7$	cohérent

Seul **b)** est certainement faux (le bon résultat est 1 514 083). Pour a) et c), la preuve par 9 ne permet pas de conclure.

Le résultat c) s'obtient à partir du produit exact 1 544 326 en **permutant** deux chiffres : la somme des chiffres, donc le reste modulo 9, ne change pas. La preuve par 9 ne détecte jamais une permutation de chiffres, ni le remplacement d'un 0 par un 9 (ou l'inverse), ni plus généralement une erreur qui modifie le résultat d'un multiple de 9.

3. Modulo 11 : $2347 \equiv 7 - 4 + 3 - 2 = 4$, $658 \equiv 8 - 5 + 6 = 9$, et $4 \times 9 = 36 \equiv 3$; mais $1\,544\,236 \equiv 6 - 3 + 2 - 4 + 4 - 5 + 1 = 1$. Comme $3 \not\equiv 1$ [11], la preuve par 11 **détecte l'erreur**. Pour 1 544 326 : somme des chiffres $25 \equiv 7$ [9] ✓ et $6 - 2 + 3 - 4 + 4 - 5 + 1 = 3$ [11] ✓.

■ Corrigé de l'exercice 38

1. On multiplie le reste précédent par 4 (ou par 7) et on réduit modulo 9 :

n	0	1	2	3	4	5	6
reste de 4^n	1	4	7	1	4	7	1
reste de 7^n	1	7	4	1	7	4	1

Les restes se répètent avec la période 3 : $4^3 = 64 = 63 + 1 \equiv 1$ et $7^3 = 343 = 9 \times 38 + 1 \equiv 1$ [9], donc $4^{n+3} = 4^n \times 4^3 \equiv 4^n$ et de même $7^{n+3} \equiv 7^n$ [9].

2. $2026 = 3 \times 675 + 1$: $4^{2026} = (4^3)^{675} \times 4 \equiv 4$. $2027 = 3 \times 675 + 2$: $7^{2027} \equiv 7^2 = 49 \equiv 4$. Donc $4^{2026} + 7^{2027} \equiv 8$ [9].

3. Soit $n = 3q + r$ avec $r \in \{0, 1, 2\}$: $4^n + 7^n = 4^r + 7^r$, qui vaut 2, $11 \equiv 2$ ou $7 + 4 = 11 \equiv 2$. Dans tous les cas $4^n + 7^n \equiv 2$ [9] : $9 \mid 4^n + 7^n - 2$.

4. $4^n + 5 \equiv 0 \iff 4^n \equiv 4$ [9] $\iff n \equiv 1$ [3]. Pour $r = 0, 1, 2$: $7^r + 2 \times 4^r \equiv 3, 15 \equiv 6, 4 + 14 = 18 \equiv 0$: $9 \mid 7^n + 2 \times 4^n \iff n \equiv 2$ [3].

■ Corrigé de l'exercice 39

1. $N - N' = (100a + 10b + c) - (100c + 10b + a) = 99a - 99c = 99(a - c)$, et $99 = 9 \times 11$.

2. $k \geq 2$ par hypothèse, et $k = a - c \leq 9 - 1 = 8$. Puis $D = 99k = 100k - k = 100(k - 1) + (100 - k) = 100(k - 1) + 90 + (10 - k)$, avec $1 \leq k - 1 \leq 7$ et $2 \leq 10 - k \leq 8$: les chiffres de D sont $k - 1, 9, 10 - k$. Ainsi $D' = 100(10 - k) + 90 + (k - 1)$ et $D + D' = 100 \times 9 + 180 + 9 = 1089$, quel que soit N .

3. $\overline{aba} = 101a + 10b = 11(9a + b) + 2a - b$, donc $\overline{aba} \equiv 2a - b$ [11]. Comme $-9 \leq 2a - b \leq 18$, $11 \mid 2a - b \iff 2a - b \in \{0, 11\}$: $b = 2a$ ($a \leq 4$) ou $b = 2a - 11$ ($a \geq 6$) :

121, 242, 363, 484, 616, 737, 858, 979.

4. $\overline{abba} = 1001a + 110b = 11(91a + 10b)$. Comme $9 \wedge 11 = 1$, $99 \mid N \iff 9 \mid N \iff 9 \mid 2(a + b)$; et si $9 \mid 2s$, alors $9 \mid 5 \times 2s - 9s = s$: la condition est $9 \mid a + b$, soit $a + b \in \{9, 18\}$: 10 palindromes,

1881, 2772, 3663, 4554, 5445, 6336, 7227, 8118, 9009, 9999.

Plus généralement, si N est un palindrome à $2m$ chiffres, les rangs i et $2m - 1 - i$ des chiffres égaux sont de parités différentes : dans la somme alternée du critère par 11, les termes s'annulent deux à deux, et $11 \mid N$.

■ Corrigé de l'exercice 40

1. $76^2 = 5776 \equiv 76$ [100]. **Initialisation** : vrai pour $k = 1$. **Hérédité** : si $76^k \equiv 76$, alors $76^{k+1} = 76^k \times 76 \equiv 76^2 \equiv 76$ [100]. **Conclusion** : $76^k \equiv 76$ [100] pour tout $k \geq 1$.

2. $2^{10} = 1024 \equiv 24$, donc $2^{20} \equiv 24^2 = 576 \equiv 76$ [100]. Puis $2026 = 20 \times 101 + 6$: $2^{2026} = (2^{20})^{101} \times 2^6 \equiv 76^{101} \times 64 \equiv 76 \times 64 = 4864$. 2^{2026} se termine par 64.

3. a) Pour $n \geq 2$: $75 \times 2^n = 3 \times 25 \times 4 \times 2^{n-2} = 100 \times 3 \times 2^{n-2}$. Or $2^{20} - 1 \equiv 75$, donc $2^{n+20} - 2^n = 2^n(2^{20} - 1) \equiv 75 \times 2^n \equiv 0$ [100].

b) On double le reste précédent modulo 100 :

n	2	3	4	5	6	7	8	9	10	11
$2^n \bmod 100$	4	8	16	32	64	28	56	12	24	48
n	12	13	14	15	16	17	18	19	20	21
$2^n \bmod 100$	96	92	84	68	36	72	44	88	76	52

Ces 20 restes sont distincts, multiples de 4 et non multiples de 5 ; or il y a exactement $25 - 5 = 20$ multiples de 4 entre 0 et 99 qui ne sont pas multiples de 5 (on retire 0, 20, 40, 60, 80) : ce sont donc tous ceux-là.

c) Pour $n \geq 2$, le reste de 2^n ne dépend que de n modulo 20 (question a), et 76 n'apparaît que pour $n = 20$ dans le tableau ; enfin $2^1 = 2$. 2^n finit par 76 $\iff n \in 20\mathbb{N}^*$. 50 et 06 ne sont pas multiples de 4 : **jamais**.

■ Corrigé de l'exercice 41

1. Deux anagrammes N et M ont la même somme des chiffres : $N \equiv S(N) = S(M) \equiv M [9]$.

2. a) On double le reste précédent :

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

$2^6 \equiv 1 [9]$, donc $2^{n+6} \equiv 2^n$. Écrivons $m = 6q + r$ et $n = 6q' + r'$ ($0 \leq r, r' \leq 5$) : $2^m \equiv 2^r$ et $2^n \equiv 2^{r'}$. Les six restes 1, 2, 4, 8, 7, 5 étant distincts, $2^m \equiv 2^n [9] \iff r = r' \iff m \equiv n [6]$.

b) $S(2^n) \equiv 2^n [9]$ a pour reste 1, 2, 4, 5, 7 ou 8 modulo 9, alors qu'un multiple de 3 a pour reste 0, 3 ou 6 : **jamais un multiple de 3**. Comme $2025 = 9 \times 225$, $S(2^n) \neq 2025$.

3. a) Deux anagrammes ont le même nombre k de chiffres : $10^{k-1} \leq 2^n < 2^m < 10^k$, donc $2^m < 10 \times 10^{k-1} \leq 10 \times 2^n$, soit $2^{m-n} < 10$ et $m - n \leq 3$.

b) D'après 1, $2^m \equiv 2^n [9]$, donc $6 \mid m - n$ d'après 2a ; c'est impossible avec $1 \leq m - n \leq 3$. Deux puissances de 2 distinctes ne sont jamais anagrammes.

4. De même, $5^{m-n} < 10$ impose $m = n + 1$, puis $9 \mid 5^{n+1} - 5^n = 4 \times 5^n$. Alors le nombre premier 3 diviserait le produit $4 \times 5 \times \dots \times 5$, donc 4 ou 5 (lemme) : impossible. Pas d'anagrammes non plus.

5. $3 \times 1035 = 3105$, qui a les mêmes chiffres 0, 1, 3, 5 : un entier et son triple peuvent être anagrammes. Pour $n \geq 2$, $3^n \equiv 0 [9]$: deux puissances de 3 (à partir de 9) sont **toujours** congrues modulo 9, et la condition nécessaire de la question 1 ne fournit aucune contradiction.

■ Corrigé de l'exercice 42

1. $6 + 3 \times 1 + 1 + 3 \times 1 + 2 + 3 \times 0 + 2 + 3 \times 6 + 0 + 3 \times 5 + 1 + 3 \times 7 = 72$: il faut $72 + a_{13} \equiv 0 [10]$, d'où la clé $a_{13} = 8$ (code 6 111202 605178).

2. a)

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

 : les dix restes sont distincts.

b) Seul le terme $w a_i$ devient $w b$: S devient $S' = S + w d$ avec $d = b - a_i$ et $1 \leq |d| \leq 9$. Si $w = 1$, $10 \nmid d$. Si $w = 3$, soit $p \in \{1, \dots, 9\}$ le reste de d modulo 10 : $3d \equiv 3p \not\equiv 0 [10]$ d'après le tableau. Dans les deux cas $S' \neq 0$: **l'erreur est détectée**.

3. Les rangs i et $i + 1$ ont les poids w et w' , égaux à 1 et 3 dans un ordre ou dans l'autre. S est modifié de $(wy + w'x) - (wx + w'y) = (w - w')(y - x) = \pm 2(y - x)$. Or $10 \mid 2(x - y) \iff 5 \mid x - y$, et $1 \leq |x - y| \leq 9$: **détectée $\iff |x - y| \neq 5$** . Exemple : échanger $a_9 = 0$ et $a_{10} = 5$ donne 6 111202 650178, accepté par le lecteur (S diminue de 10).

4. Après l'échange, la somme est modifiée de $(i a_j + j a_i) - (i a_i + j a_j) = (j - i)(a_i - a_j)$. Par l'absurde, si 11 divisait ce produit, comme 11 est premier, il diviserait $j - i$ ou $a_i - a_j$ (lemme) ; impossible car $1 \leq j - i \leq 9$ et $1 \leq |a_i - a_j| \leq 10$. **L'échange est toujours détecté** : c'est l'intérêt d'un module premier.

32

Corrigés : nombres premiers

■ Corrigé de l'exercice 43

1. $22^2 = 484 < 487 < 529 = 23^2$: on teste les premiers $p \leq 22$. 487 est impair, de somme des chiffres 19, ne finit ni par 0 ni par 5 ; et $487 = 7 \times 69 + 4 = 11 \times 44 + 3 = 13 \times 37 + 6 = 17 \times 28 + 11 = 19 \times 25 + 12$. Aucun diviseur premier $p \leq \sqrt{487}$: **487 est premier**.

Pour 779 ($27^2 < 779 < 28^2$), on trouve en testant 2, 3, ..., 19 : **$779 = 19 \times 41$** , qui n'est pas premier.

2. $899 = 900 - 1 = 30^2 - 1^2 = (30 - 1)(30 + 1) = \mathbf{29 \times 31}$; $1599 = 40^2 - 1^2 = 39 \times 41 = \mathbf{3 \times 13 \times 41}$; $9991 = 10\,000 - 9 = 100^2 - 3^2 = \mathbf{97 \times 103}$ (97 et 103 sont premiers : aucun diviseur premier ≤ 10).
3. $100^3 + 3^3 = 1\,000\,000 + 27 = 1\,000\,027$, donc $1\,000\,027 = (100 + 3)(100^2 - 300 + 9) = 103 \times 9709$. Puis $9709 = 7 \times 1387$ et, en testant les premiers $p \leq 37$, $1387 = 19 \times 73$. Comme 7, 19, 73, 103 sont premiers :

$$\mathbf{1\,000\,027 = 7 \times 19 \times 73 \times 103}.$$

■ Corrigé de l'exercice 44

1. On lit **2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31**. Pour $n \geq 2$, 1 et n sont deux diviseurs distincts : $d(n) = 2$ signifie qu'il n'y en a pas d'autre, c'est la définition d'un nombre premier (et $d(1) = 1$).
2. $d(n) = 3$ pour **4, 9, 25**, et $d(n) = 5$ pour **16**. Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors $(\alpha_1 + 1) \cdots (\alpha_k + 1) = 3$ (ou 5), nombre premier : un seul facteur, $k = 1$ et $\alpha_1 = 2$ (ou 4) ; réciproquement $d(p^2) = 3$ et $d(p^4) = 5$. Après $2^4 = 16$, le plus petit est **$3^4 = 81$** .
3. $(\alpha_1 + 1) \cdots (\alpha_k + 1) = 4$ avec des facteurs ≥ 2 : soit un facteur égal à 4 ($n = p^3$), soit deux facteurs égaux à 2 ($n = pq$) ; la réciproque se vérifie par la formule. Pour $n \leq 36$: 8, 27 et 2×3 , 2×5 , 2×7 , 2×11 , 2×13 , 2×17 , 3×5 , 3×7 , 3×11 , 5×7 :

$$\mathbf{6, 8, 10, 14, 15, 21, 22, 26, 27, 33, 34, 35} \quad (12 \text{ entiers, conformes au diagramme}).$$

Le record est $d(36) = 9$, avec $36 = 2^2 \times 3^2$ et $(2 + 1)(2 + 1) = 9$; viennent ensuite $24 = 2^3 \times 3$ et $30 = 2 \times 3 \times 5$, avec $(3 + 1)(1 + 1) = (1 + 1)^3 = 8$ diviseurs.

■ Corrigé de l'exercice 45

1. $2160 = 2^4 \times 3^3 \times 5$. Ses diviseurs sont les $2^\alpha 3^\beta 5^\gamma$ avec $0 \leq \alpha \leq 4$, $0 \leq \beta \leq 3$, $0 \leq \gamma \leq 1$:
 $d(N) = 5 \times 4 \times 2 = \boxed{40}$.

Pairs ($\alpha \geq 1$) : $4 \times 4 \times 2 = \boxed{32}$; impairs ($\alpha = 0$) : $\boxed{8}$; multiples de 30 = $2 \times 3 \times 5$ ($\alpha \geq 1$, $\beta \geq 1$, $\gamma = 1$) : $4 \times 3 \times 1 = \boxed{12}$; carrés ($\alpha \in \{0, 2, 4\}$, $\beta \in \{0, 2\}$, $\gamma = 0$) : $3 \times 2 = \boxed{6}$, à savoir 1, 4, 9, 16, 36, 144.

Les diviseurs impairs sont ceux de $3^3 \times 5 = 135$: leur somme est $(1 + 3 + 9 + 27)(1 + 5) = \boxed{240}$.

2. Un diviseur impair de n n'a pas le facteur 2 dans sa décomposition : c'est un diviseur de m . Si $m = \prod p_i^{\alpha_i}$ (les p_i impairs), alors $n = 2^a \prod p_i^{\alpha_i}$ et $2n = 2^{a+1} \prod p_i^{\alpha_i}$, donc

$$d(2n) - d(n) = (a+2)d(m) - (a+1)d(m) = \boxed{d(m)}.$$

Pour $n = 2160$: $d(4320) = d(2^5 \times 3^3 \times 5) = 6 \times 4 \times 2 = 48 = 40 + 8 \checkmark$.

3. $d(n) = (a+1)(b+1)$, $d(2n) = (a+2)(b+1)$ et $d(3n) = (a+1)(b+2)$. Les conditions s'écrivent $b+1 = 4$ et $a+1 = 6$: $a = 5$, $b = 3$, $n = 2^5 \times 3^3 = 864$. Vérification : $d(864) = 24$, $d(1728) = d(2^6 \times 3^3) = 28$, $d(2592) = d(2^5 \times 3^4) = 30 \checkmark$.

■ Corrigé de l'exercice 46

1. Comme $p \geq 5$ est premier, $p \equiv 1$ ou $5 \pmod{6}$. Si $p \equiv 1 \pmod{6}$, alors $p+2 \equiv 3 \pmod{6}$, donc $3 \mid p+2$ avec $p+2 > 3$: $p+2$ ne serait pas premier. Donc $p \equiv 5 \pmod{6}$, $p+1 = 6k$, et $p+(p+2) = 2(p+1) = \boxed{12k}$.
2. Pour $p = 5$: 29 et 31 sont premiers. Si $p \neq 5$, alors $5 \nmid p$ et $p^2 \equiv 1$ ou $4 \pmod{5}$ (tableau de l'exercice 34). Si $p^2 \equiv 1$, $5 \mid p^2+4$; si $p^2 \equiv 4$, $5 \mid p^2+6$; dans les deux cas c'est un multiple de 5 strictement supérieur à 5, non premier. $\boxed{p = 5}$ (et 29, 31 sont jumeaux).
3. Si $q = p+2$: $pq+1 = p^2+2p+1 = (p+1)^2$. Réciproquement, si $pq+1 = m^2$ ($m \in \mathbb{N}$), alors $m \geq 3$ et $pq = (m-1)(m+1)$. Par unicité de la décomposition, les diviseurs positifs de pq sont 1, p , q , pq ; comme $m-1 < m+1$, on a $m-1 = 1$ (exclu car $m \geq 3$) ou $m-1 = p$ et $m+1 = q$. Donc $\boxed{q = p+2}$.

Pour $p \neq 5$, $5p+1$ est un carré si et seulement si p et 5 sont jumeaux, soit $p \in \{3, 7\}$; et $5 \times 5 + 1 = 26$ n'est pas un carré (en général $p^2 < p^2 + 1 < (p+1)^2$). $\boxed{p \in \{3, 7\}}$ (16 et 36). Pour $23p+1$: 21 et 25 ne sont pas premiers : $\boxed{\text{aucun}}$.

■ Corrigé de l'exercice 47

1. Si $\sigma(a) - a = b$ et $\sigma(b) - b = a$, alors $\sigma(a) = a + b = \sigma(b)$; réciproquement, $\sigma(a) = a + b$ donne $\sigma(a) - a = b$, et de même pour b .

$220 = 2^2 \times 5 \times 11$ et $284 = 2^2 \times 71$ (71 est premier). $\sigma(220) = 7 \times 6 \times 12 = 504$ et $\sigma(284) = 7 \times 72 = 504 = 220 + 284$: $\boxed{220 \text{ et } 284 \text{ sont amiables}}$.

2. a) Pour $n \geq 2$, $3 \times 2^{n-1}$, 3×2^n et $9 \times 2^{2n-1}$ sont pairs : p, q, r sont impairs. De plus $q = 2p+1 > p$ et $r - q = 9 \times 2^{2n-1} - 3 \times 2^n = 3 \times 2^n (3 \times 2^{n-1} - 1) = 3 \times 2^n p > 0$.

b) 2, p, q sont des nombres premiers distincts, donc

$$\sigma(2^n pq) = (2^{n+1} - 1)(p+1)(q+1) = (2^{n+1} - 1) \times 3 \times 2^{n-1} \times 3 \times 2^n = 9 \times 2^{2n-1} (2^{n+1} - 1)$$

et $\sigma(2^n r) = (2^{n+1} - 1)(r+1) = (2^{n+1} - 1) \times 9 \times 2^{2n-1}$: c'est le même nombre.

c) $pq = 9 \times 2^{2n-1} - 3 \times 2^{n-1} - 3 \times 2^n + 1 = 9 \times 2^{2n-1} - 9 \times 2^{n-1} + 1$, donc $pq + r = 18 \times 2^{2n-1} - 9 \times 2^{n-1} = 9 \times 2^{n-1} (2^{n+1} - 1)$ et

$$A + B = 2^n(pq + r) = 9 \times 2^{2n-1} (2^{n+1} - 1) = \sigma(A) = \sigma(B).$$

Enfin $A \neq B$ car $pq - r = 2 - 9 \times 2^{n-1} \neq 0$. D'après 1, A et B sont amiables.

3. a) $n = 2$: $p = 5$, $q = 11$, $r = 71$, premiers ; $A = 4 \times 55 = 220$ et $B = 4 \times 71 = 284$.

b) $n = 3$: $p = 11$ et $q = 23$ sont premiers, mais $r = 287 = 7 \times 41$ ne l'est pas (d'ailleurs 2024 et 2296 ne sont pas amiables : $\sigma(2296) = 5040 \neq 4320$).

c) $n = 4$: $p = 23$, $q = 47$, $r = 1151$. Comme $33^2 < 1151 < 34^2$, on teste 2, 3, 5, ..., 31 : les restes de 1151 par 3, 7, 11, 13, 17, 19, 23, 29, 31 sont 2, 3, 7, 7, 12, 11, 1, 20, 4 : 1151 est premier.

$A = 2^4 \times 23 \times 47 = 17\,296$ et $B = 2^4 \times 1151 = 18\,416$ sont amiables.

■ Corrigé de l'exercice 48

1. $(6k+1)(6l+1) = 6(6kl+k+l)+1$. Par récurrence sur le nombre de facteurs (ou par compatibilité : $1 \times 1 \equiv 1 [6]$), un produit de tels entiers est congru à 1 modulo 6.

2. a) $N = 6k + 5 = 2(3k + 2) + 1 = 3(2k + 1) + 2$: les restes de N par 2 et par 3 sont 1 et 2, donc $2 \nmid N$ et $3 \nmid N$.

b) Un diviseur premier p de N est donc différent de 2 et de 3 : $p \geq 5$ et $p \equiv 1$ ou $5 [6]$. *Par l'absurde* : si tous les facteurs premiers de $N = p_1 p_2 \dots p_k$ (répétés selon leur exposant) étaient congrus à 1 modulo 6, alors $N \equiv 1 [6]$ d'après 1, alors que $N \equiv 5 [6]$. **N a un diviseur premier $p \equiv 5 [6]$.**

3. a) Pour $n \geq 3$, $6 = 1 \times 2 \times 3$ divise $n!$, donc $N \equiv -1 \equiv 5 [6]$, et $N \geq 5$. Si un premier $p \leq n$ divisait N , comme il divise $n!$ (c'est l'un des facteurs), il diviserait $n! - N = 1$: impossible.

b) D'après 2b, N a un diviseur premier $p \equiv 5 [6]$, et $p > n$ d'après a). *Par l'absurde*, s'il n'y avait qu'un nombre fini de premiers de la forme $6k - 1$, on choisirait $n \geq 3$ supérieur à tous : contradiction. Il y a une infinité de nombres premiers de la forme $6k - 1$.

4. $(4k+1)(4l+1) = 4(4kl+k+l)+1$: un produit d'entiers $\equiv 1 [4]$ est $\equiv 1 [4]$. Un entier $N \equiv 3 [4]$ est impair, ses diviseurs premiers sont impairs, donc $\equiv 1$ ou $3 [4]$, et l'un d'eux au moins est $\equiv 3 [4]$. Pour $n \geq 4$, $4 \mid n!$, donc $N = n! - 1 \equiv 3 [4]$, et ses diviseurs premiers sont $> n$: infinité de premiers de la forme $4k + 3$.

Exemple : $5! - 1 = 119 = 7 \times 17$; $7 \equiv 3 [4]$ et $17 \equiv 5 [6]$ sont bien supérieurs à 5 (ce ne sont pas les mêmes !).

Pour la forme $6k + 1$: $5 \times 11 = 55 \equiv 1 [6]$ alors que 5 et 11 sont $\equiv 5 [6]$: un entier $\equiv 1 [6]$ peut n'avoir **aucun** diviseur premier $\equiv 1 [6]$. L'argument de la question 2 ne fonctionne plus (le résultat reste vrai, mais demande d'autres outils).

33

Corrigés : PGCD et PPCM■ **Corrigé de l'exercice 49**

1. On applique le lemme $a \wedge b = b \wedge r$ (où r est le reste de a par b) jusqu'à obtenir un reste nul :

dividende	7470	4770	2700	2070	630	180
diviseur	4770	2700	2070	630	180	90
quotient	1	1	1	3	3	2
reste	2700	2070	630	180	90	0

Ainsi $7470 \wedge 4770 = 4770 \wedge 2700 = \dots = 180 \wedge 90 = 90 \wedge 0$: le dernier reste non nul donne $d = 90$.

2. $a \vee b = \frac{ab}{a \wedge b} = \frac{7470 \times 4770}{90} = 7470 \times 53 = 395\,910$. Comme $a = 90 \times 83$ et $b = 90 \times 53$, avec $83 \wedge 53 = 1$ (car d est le PGCD) : $\frac{b}{a} = \frac{53}{83}$.

3. $7470 = 2 \times 3^2 \times 5 \times 83$ et $4770 = 2 \times 3^2 \times 5 \times 53$ (53 et 83 sont premiers : aucun premier $p \leq 7$ ne les divise et $11^2 > 83$). Plus petits exposants : $d = 2 \times 3^2 \times 5 = 90$; plus grands exposants : $a \vee b = 2 \times 3^2 \times 5 \times 53 \times 83 = 395\,910$ ✓.

4. Les diviseurs communs à a et b sont les diviseurs de $d = 2 \times 3^2 \times 5$: il y en a $(1+1)(2+1)(1+1) = 12$ dans $\mathbb{N}$, à savoir 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90, et 24 dans $\mathbb{Z}$ (avec leurs opposés).

5. a) ka est un carré si et seulement si tous les exposants de sa décomposition sont pairs. Les exposants de 2, 5 et 83 dans a valent 1 : chacun doit apparaître dans k avec un exposant impair, donc $2 \times 5 \times 83 = 830$ divise k . Inversement $830a = 2^2 \times 3^2 \times 5^2 \times 83^2 = 2490^2$: $k = 830$.

b) $b \mid na \iff 90 \times 53 \mid 90 \times 83n \iff 53 \mid 83n$. Le nombre premier 53 ne divise pas 83, donc (lemme d'Euclide) $53 \mid 83n \iff 53 \mid n$: $n = 53$. Et $53a = 395\,910 = a \vee b$: c'est normal, na doit être un multiple commun de a et b .

■ **Corrigé de l'exercice 50**

Dans chaque cas, on pose $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$ et $a' \leq b'$; alors $a \vee b = da'b'$.

1. $d = 14$ et $ab = 196$ $a'b' = 11\,760$, donc $a'b' = 60 = 2^2 \times 3 \times 5$. Les couples (a', b') premiers entre eux de produit 60 sont (1, 60), (3, 20), (4, 15), (5, 12) (on exclut (2, 30) et (6, 10)). Réciproquement, ces couples conviennent ($a \wedge b = 14(a' \wedge b') = 14$) : (14, 840), (42, 280), (56, 210), (70, 168).

2. $a \vee b = da'b' = 10d$, donc $a'b' = 10$: $(a', b') \in \{(1, 10), (2, 5)\}$. Puis $a + b = d(a' + b') = 189$: pour (1, 10), $11d = 189$ est impossible ($11 \nmid 189$) ; pour (2, 5), $7d = 189$, $d = 27$. $(a, b) = (54, 135)$ (contrôle : $54 \wedge 135 = 27$, $54 \vee 135 = 270 = 10 \times 27$ ✓).

3. Ici $a' < b'$ et $36(b'^2 - a'^2) = 756$, soit $(b' - a')(b' + a') = 21$ avec $0 < b' - a' < b' + a'$: $b' - a' = 1$, $b' + a' = 21$ donne $(a', b') = (10, 11)$; $b' - a' = 3$, $b' + a' = 7$ donne $(a', b') = (2, 5)$. Ces couples sont premiers entre eux : $(a, b) \in \{(60, 66), (12, 30)\}$ ($66^2 - 60^2 = 6 \times 126 = 756$ ✓).

■ Corrigé de l'exercice 51

- $(2n + 11)(2n + 1) = 4n^2 + 24n + 11$ et $4B = 4n^2 + 24n + 44$: la différence vaut bien $\boxed{33}$. Comme $d \mid A$ et $d \mid B$, d divise la combinaison $4B - (2n + 11)A = 33$: $d \in \{1, 3, 11, 33\}$.
- a) Tableau des restes modulo 3 : si $n \equiv 0, 1, 2$, alors $A \equiv 1, 0, 2$. Donc $3 \mid A \iff n \equiv 1 [3]$, et alors $B \equiv 1 + 6 + 11 = 18 \equiv 0 [3]$.
b) Modulo 11, $A \equiv 0 \iff 2n \equiv -1 \equiv 10$; les restes de $2n$ pour $n \equiv 0, 1, \dots, 10$ sont 0, 2, 4, 6, 8, 10, 1, 3, 5, 7, 9 : $11 \mid A \iff n \equiv 5 [11]$, et alors $B \equiv 25 + 30 + 11 = 66 \equiv 0 [11]$.
c) $3 \mid d \iff (3 \mid A \text{ et } 3 \mid B) \iff n \equiv 1 [3]$, et de même $11 \mid d \iff n \equiv 5 [11]$. Si $3 \mid d$ et $11 \mid d$, alors $33 \mid d$ ($3 \wedge 11 = 1$). Comme $d \mid 33$:

	$n \equiv 5 [11]$	$n \not\equiv 5 [11]$
$n \equiv 1 [3]$	$d = 33$	$d = 3$
$n \not\equiv 1 [3]$	$d = 11$	$d = 1$

(Les deux conditions réunies équivalent à $n \equiv 16 [33]$: parmi 5, 16, 27, seul 16 est $\equiv 1 [3]$.)
 $n = 5$: $A = 11$, $B = 66$, $\boxed{d = 11}$. $n = 16$: $A = 33$, $B = 363 = 11 \times 33$, $\boxed{d = 33}$. $n = 2026 = 3 \times 675 + 1 = 11 \times 184 + 2$: $\boxed{d = 3}$. $n = 2027$: $n \equiv 2 [3]$ et $n \equiv 3 [11]$, $\boxed{d = 1}$.

- $\frac{B}{A}$ est irréductible $\iff d = 1 \iff \boxed{n \not\equiv 1 [3] \text{ et } n \not\equiv 5 [11]}$ (c'est le cas pour $n = 2027$).
- Condition nécessaire. Si $A \mid B$, alors $A \mid 4B$ et $A \mid (2n + 11)A$, donc $A \mid 33$: $2n + 1 \in \{\pm 1, \pm 3, \pm 11, \pm 33\}$, soit $n \in \{-17, -6, -2, -1, 0, 1, 5, 16\}$. Vérification :

n	-17	-6	-2	-1	0	1	5	16
A	-33	-11	-3	-1	1	3	11	33
B	198	11	3	6	11	18	66	363
B/A	-6	-1	-1	-6	11	6	6	11

$$\boxed{\frac{B}{A} \in \mathbb{Z} \iff n \in \{-17, -6, -2, -1, 0, 1, 5, 16\}}$$

C'était prévisible : si $A \mid 33$, chaque nombre premier (3 ou 11) qui divise A divise aussi B (question 2), et 33 n'a pas de facteur carré.

■ Corrigé de l'exercice 52

- Soit δ un diviseur de n . Si $\delta \mid k$, alors δ divise la combinaison $n - k$; si $\delta \mid n - k$, alors $\delta \mid n - (n - k) = k$: ainsi $\delta \mid k \iff \delta \mid n - k$. Donc k et n d'une part, $n - k$ et n d'autre part, ont les **mêmes diviseurs communs**, et $\boxed{k \wedge n = (n - k) \wedge n}$. Enfin $1 \leq k \leq n - 1 \iff 1 \leq n - k \leq n - 1$: $k \in I_n \iff n - k \in I_n$.
- Par l'absurde, si $k = n - k$ avec $k \in I_n$, alors $n = 2k$ et $k \wedge n = k \wedge 2k = k$, donc $k = 1$ et $n = 2$: exclu. Les éléments de I_n se groupent donc par paires $\{k, n - k\}$ de deux éléments distincts : $\boxed{N_n \text{ est pair}}$. Chaque paire apporte $\frac{k}{n} + \frac{n-k}{n} = 1$, et il y a $\frac{N_n}{2}$ paires : $\boxed{S_n = \frac{N_n}{2}}$.
- Le seul facteur premier de p^a est p , donc $k \wedge p^a = 1 \iff p \nmid k$. Parmi $1, \dots, p^a - 1$, les multiples de p sont $p, 2p, \dots, (p^{a-1} - 1)p$: il y en a $p^{a-1} - 1$. Donc $N_{p^a} = (p^a - 1) - (p^{a-1} - 1) = \boxed{p^a - p^{a-1}}$.
 $1024 = 2^{10}$: $N = 1024 - 512 = \boxed{512}$, $S = \boxed{256}$. $343 = 7^3$: $N = 343 - 49 = \boxed{294}$, $S = \boxed{147}$.

4. $k \wedge pq = 1 \iff p \nmid k \text{ et } q \nmid k$. Parmi $1, \dots, pq - 1$, il y a $q - 1$ multiples de p et $p - 1$ multiples de q , et aucun multiple commun : si $p \mid k$ et $q \mid k$, alors $pq \mid k$ ($p \wedge q = 1$), impossible pour $1 \leq k < pq$. Donc $N_{pq} = pq - 1 - (q - 1) - (p - 1) = (p - 1)(q - 1)$.

1013 est premier : $31^2 < 1013 < 32^2$ et $1013 = 3 \times 337 + 2 = 7 \times 144 + 5 = 11 \times 92 + 1 = 13 \times 77 + 12 = 17 \times 59 + 10 = 19 \times 53 + 6 = 23 \times 44 + 1 = 29 \times 34 + 27 = 31 \times 32 + 21$ (ni 2 ni 5). Avec $2026 = 2 \times 1013$: $N_{2026} = 1012$, $S_{2026} = 506$. Avec $2021 = 43 \times 47$: $N_{2021} = 42 \times 46 = 1932$, $S_{2021} = 966$.

■ Corrigé de l'exercice 53

1. Par l'absurde, supposons $(a' + b') \wedge a'b' \neq 1$: ce PGCD admet un diviseur premier p , qui divise $a' + b'$ et $a'b'$. D'après le lemme d'Euclide, $p \mid a'$ ou $p \mid b'$. Si $p \mid a'$, alors $p \mid (a' + b') - a' = b'$; si $p \mid b'$, de même $p \mid a'$. Dans les deux cas p divise $a' \wedge b' = 1$: contradiction. Donc $(a' + b') \wedge a'b' = 1$.
2. Soit $d = a \wedge b$, $a = da'$, $b = db'$, $a' \wedge b' = 1$; alors $a + b = d(a' + b')$ et $a \vee b = da'b'$. Par la propriété $(kx) \wedge (ky) = k(x \wedge y)$ et la question 1 : $(a + b) \wedge (a \vee b) = d((a' + b') \wedge a'b') = d = a \wedge b$.
3. a) D'après 2, $d = 276 \wedge 1440$. Or $276 = 2^2 \times 3 \times 23$ et $1440 = 2^5 \times 3^2 \times 5$: $d = 12$. Alors $a' + b' = \frac{276}{12} = 23$ et $a'b' = \frac{1440}{12} = 120$: a' et b' sont les racines de $t^2 - 23t + 120 = 0$, de discriminant $529 - 480 = 49$, soit $t = \frac{23 \pm 7}{2} \in \{8, 15\}$. Avec $8 \wedge 15 = 1$: $(a, b) \in \{(96, 180), (180, 96)\}$. Réciproquement $96 + 180 = 276$ et $96 \vee 180 = 2^5 \times 3^2 \times 5 = 1440$ ✓.
b) S'il existait un tel couple, on aurait $d = 60 \wedge 84 = 12$, $a' + b' = 5$ et $a'b' = 7$; or $t^2 - 5t + 7 = 0$ a un discriminant $25 - 28 < 0$: **aucun couple**.
4. a) Supposons $\frac{a}{b} + \frac{b}{a} = k \in \mathbb{Z}$, soit $a^2 + b^2 = kab$; avec $a = da'$, $b = db'$: $a'^2 + b'^2 = ka'b'$, d'où $a'^2 = b'(ka' - b')$ et $b' \mid a'^2$. Par l'absurde, si $b' \geq 2$, un nombre premier p divise b' , donc a'^2 , donc a' (lemme d'Euclide) : il divise $a' \wedge b' = 1$, contradiction. Donc $b' = 1$, de même $a' = 1$, et $a = b$ (alors $k = 2$).
b) Écrivons $x = \frac{p}{q}$ irréductible, $p \in \mathbb{Z}^*$, $q \in \mathbb{N}^*$. Si $x + \frac{1}{x} \in \mathbb{Z}$, alors $\frac{|p|}{q} + \frac{q}{|p|} = \pm \left(x + \frac{1}{x}\right) \in \mathbb{Z}$, donc $|p| = q$ d'après a) ; comme $p \wedge q = 1$, $q = 1$. Réciproquement $\pm 1 \pm 1 = \pm 2 \in \mathbb{Z}$: $x \in \{-1, 1\}$.

■ Corrigé de l'exercice 54

1. Notons $\alpha = v_p(a)$, $\beta = v_p(b)$, $\gamma = v_p(c)$. D'après les formules du cours : $v_p((a \wedge b) \wedge c) = \min(\min(\alpha, \beta), \gamma) = \min(\alpha, \beta, \gamma)$, et de même pour le maximum. Comme $\min(\alpha, \min(\beta, \gamma))$ a la même valeur, $(a \wedge b) \wedge c$ et $a \wedge (b \wedge c)$ ont les mêmes exposants pour tout p : ils sont égaux (unicité de la décomposition). Enfin $\delta \in \mathbb{N}^*$ divise a, b et $c \iff v_p(\delta) \leq \min(\alpha, \beta, \gamma)$ pour tout $p \iff \delta \mid a \wedge b \wedge c$.
2. Les deux membres sont symétriques en x, y, z : on peut supposer $x \leq y \leq z$. Alors le membre de gauche vaut $z + x + y + x$ et celui de droite $x + y + z + x$: **égalité**.
3. Appliquons 2 aux exposants α, β, γ d'un nombre premier p : le membre de gauche est l'exposant de p dans $(a \vee b \vee c)(a \wedge b)(b \wedge c)(c \wedge a)$, celui de droite son exposant dans $abc(a \wedge b \wedge c)$. Ces deux entiers ont les mêmes exposants pour tout p : $(a \vee b \vee c)(a \wedge b)(b \wedge c)(c \wedge a) = abc(a \wedge b \wedge c)$.
4. Euclide : $56 = 40 \times 1 + 16$, $40 = 16 \times 2 + 8$, $16 = 8 \times 2$, donc $40 \wedge 56 = 8$; $140 = 56 \times 2 + 28$, $56 = 28 \times 2$, donc $56 \wedge 140 = 28$; $140 = 40 \times 3 + 20$, $40 = 20 \times 2$, donc $140 \wedge 40 = 20$; enfin $140 = 8 \times 17 + 4$,

$8 = 4 \times 2$, donc $40 \wedge 56 \wedge 140 = 8 \wedge 140 = 4$. D'après 3 :

$$40 \vee 56 \vee 140 = \frac{40 \times 56 \times 140 \times 4}{8 \times 28 \times 20} = \frac{1\,254\,400}{4480} = \boxed{280}.$$

Vérification : $40 = 2^3 \times 5$, $56 = 2^3 \times 7$, $140 = 2^2 \times 5 \times 7$, d'où le PPCM $2^3 \times 5 \times 7 = 280$ ✓.

5. Posons $g = a \wedge b \wedge c$. ($\Leftarrow$) Si $a \wedge b = b \wedge c = c \wedge a = 1$, alors $g = 1$ (il divise $a \wedge b$) et la formule 3 donne $a \vee b \vee c = abc$. ($\Rightarrow$) Si $a \vee b \vee c = abc$, la formule 3 donne $(a \wedge b)(b \wedge c)(c \wedge a) = g$. Or g divise chacun des trois PGCD, qui sont donc $\geq g : g \geq g^3$, d'où $g = 1$, puis $(a \wedge b)(b \wedge c)(c \wedge a) = 1$ et les trois PGCD valent 1. **Équivalence démontrée.**

$6 \wedge 10 \wedge 15 = 2 \wedge 15 = 1$, mais $\boxed{6 \vee 10 \vee 15 = 30} \neq 900 = 6 \times 10 \times 15$: la condition $a \wedge b \wedge c = 1$ ne suffit pas ($6 \wedge 10 = 2$) ; il faut des nombres premiers entre eux **deux à deux**.

6. Il suffit de vérifier, pour des réels x, y, z (puis de l'appliquer aux exposants de chaque p), que

$$\min(\max(x, y), z) = \max(\min(x, z), \min(y, z)).$$

Par symétrie en x et y , supposons $x \leq y$: alors $\min(x, z) \leq \min(y, z)$, et les deux membres valent $\min(y, z)$. D'où $\boxed{(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)}$ (ex. : $(4 \vee 6) \wedge 10 = 12 \wedge 10 = 2 = 2 \vee 2$).

34

Corrigés : équations en entiers

■ Corrigé de l'exercice 55

1. $(x+1)(y+1) = xy + x + y + 1$, donc l'équation équivaut à $(x+1)(y+1) = 42$. Pour $(x, y) \in \mathbb{N}^2$, $x+1$ et $y+1$ sont des diviseurs positifs de $42 = 2 \times 3 \times 7$, qui en a 8 : 1, 2, 3, 6, 7, 14, 21, 42. Chaque choix de $x+1$ fixe $y+1 = \frac{42}{x+1}$:

$$S = \{(0, 41), (1, 20), (2, 13), (5, 6), (6, 5), (13, 2), (20, 1), (41, 0)\}.$$

2. $(x-5)(y-3) = xy - 3x - 5y + 15$, donc l'équation équivaut à $\boxed{(x-5)(y-3) = 16}$. On parcourt les 10 diviseurs de 16 dans $\mathbb{Z}$:

$x-5$	1	2	4	8	16	-1	-2	-4	-8	-16
$y-3$	16	8	4	2	1	-16	-8	-4	-2	-1
(x, y)	(6, 19)	(7, 11)	(9, 7)	(13, 5)	(21, 4)	(4, -13)	(3, -5)	(1, -1)	(-3, 1)	(-11, 2)

Dix solutions (par exemple $9 \times 7 = 63 = 27 + 35 + 1$ ✓).

3. Le jardin et l'allée forment un rectangle $(x+2) \times (y+2)$; l'aire de l'allée vaut $(x+2)(y+2) - xy = 2x + 2y + 4$. La condition s'écrit $xy = 2x + 2y + 4$, soit $xy - 2x - 2y + 4 = 8$: $\boxed{(x-2)(y-2) = 8}$. Si $x = 1$, $-(y-2) = 8$ donne $y = -6$; si $x = 2$, $0 = 8$: impossible. Donc $1 \leq x-2 \leq y-2$, et $(x-2, y-2) \in \{(1, 8), (2, 4)\}$: **jardin de 3×10 ou de 4×6** (allées d'aire $5 \times 12 - 30 = 30$ et $6 \times 8 - 24 = 24$ ✓).

■ Corrigé de l'exercice 56

1. $(x-y)(x+y) = 105$ avec $x+y > 0$, donc $x-y > 0$, et $y = 0$ est exclu (105 n'est pas un carré) : $0 < x-y < x+y$. Comme $105 = 3 \times 5 \times 7$, $(x-y, x+y) \in \{(1, 105), (3, 35), (5, 21), (7, 15)\}$; ces facteurs sont impairs, donc $x = \frac{(x-y)+(x+y)}{2}$ et $y = \frac{(x+y)-(x-y)}{2}$ sont entiers : $S = \{(53, 52), (19, 16), (13, 8), (11, 4)\}$.
2. Pythagore : $x^2 = y^2 + 400$, soit $(x-y)(x+y) = 400$ avec $0 < x-y < x+y$. Comme $(x-y) + (x+y) = 2x$ est pair, les deux facteurs ont la même parité ; leur produit étant pair, **ils sont pairs** : $x-y = 2u$, $x+y = 2v$, $uv = 100$, $u < v$, d'où $(u, v) \in \{(1, 100), (2, 50), (4, 25), (5, 20)\}$ et $x = u + v$, $y = v - u$:

$$(20, 99, 101), \quad (20, 48, 52), \quad (20, 21, 29), \quad (20, 15, 25)$$

(par exemple $20^2 + 21^2 = 400 + 441 = 841 = 29^2$ ✓ ; (10, 10) donnerait $y = 0$).

3. L'équation ne change pas si l'on remplace x par $-x$ ou y par $-y$: cherchons d'abord les solutions dans $\mathbb{N}^2$. $(x-2y)(x+2y) = 33$ avec $x+2y > 0$, donc $0 < x-2y \leq x+2y$: $(x-2y, x+2y) \in \{(1, 33), (3, 11)\}$, d'où $x = \frac{1+33}{2} = 17$, $y = \frac{33-1}{4} = 8$, ou $x = 7$, $y = 2$. $S = \{(\pm 17, \pm 8), (\pm 7, \pm 2)\}$ (huit couples ; $289 - 256 = 33$ ✓).

■ Corrigé de l'exercice 57

	y modulo 5	0	1	2	3	4
1. a)	y^2 modulo 5	0	1	4	4	1
	$3y^2$ modulo 5	0	3	2	2	3

b) *Par l'absurde*, soit (x, y) une solution. Modulo 5 : $15x^2 \equiv 0$, $-7y^2 \equiv 3y^2$ et $9 \equiv 4$, donc $3y^2 \equiv 4$ [5]. D'après le tableau, $3y^2$ n'est jamais congru à 4 modulo 5 : contradiction. **Aucune solution.**

2. a) $4^3 = 64 = 3 \times 21 + 1$: $4^3 \equiv 1$ [21]. Si $x = 3q + r$ ($0 \leq r \leq 2$), alors $4^x = (4^3)^q 4^r \equiv 4^r$ [21] : $4^x \equiv 1$, 4 ou 16 [21] selon que $r = 0, 1$ ou 2.

b) Une solution donnerait $4^x = 21y + 5 \equiv 5$ [21] : impossible d'après a). **Aucune solution.**

c) $4^x - 21y = 16 \iff (21 \mid 4^x - 16 \text{ et } y = \frac{4^x - 16}{21}) \iff (4^x \equiv 16 \text{ [21] et } y = \frac{4^x - 16}{21})$. D'après a) :

$$S = \left\{ \left(3q + 2, \frac{4^{3q+2} - 16}{21} \right), q \in \mathbb{N} \right\}, \text{ par exemple } (2, 0), (5, 48), (8, 3120).$$

3. a) $x^2 = 84 - 3y^2 \equiv 0$ [3]. Or si $3 \nmid x$, $x \equiv \pm 1$ et $x^2 \equiv 1$ [3] : donc $3 \mid x$, $x = 3u$, et l'équation devient $9u^2 + 3y^2 = 84$, soit $3u^2 + y^2 = 28$.

b) $y^2 = 28 - 3u^2 \leq 28$, donc $0 \leq y \leq 5$; et $y^2 \equiv 28 \equiv 1$ [3], donc $3 \nmid y$: $y \in \{1, 2, 4, 5\}$.

c) $y = 1$: $3u^2 = 27$, $u = 3$, $x = 9$; $y = 2$: $u^2 = 8$, impossible ; $y = 4$: $u^2 = 4$, $u = 2$, $x = 6$; $y = 5$: $u^2 = 1$, $x = 3$. $S = \{(9, 1), (6, 4), (3, 5)\}$ ($81 + 3 = 36 + 48 = 9 + 75 = 84$ ✓).

■ Corrigé de l'exercice 58

1. Nombre de volailles : $x + y + z = 100$; prix : $5x + 3y + \frac{z}{3} = 100$, soit $15x + 9y + z = 300$ en multipliant par 3. En soustrayant la première égalité : $14x + 8y = 200$, donc $7x + 4y = 100$.
2. a) Modulo 4 : $7 \equiv 3$ et $100 \equiv 0$, donc $3x \equiv 0$ [4]. Les restes de $3x$ pour $x \equiv 0, 1, 2, 3$ sont 0, 3, 2, 1 : $3x \equiv 0$ [4] $\iff x \equiv 0$ [4].
b) $x = 4k$ ($k \in \mathbb{N}$) donne $28k + 4y = 100$, soit $y = 25 - 7k$, et $y \geq 0 \iff k \leq 3$. Réciproquement ces couples conviennent : $(x, y) \in \{(0, 25), (4, 18), (8, 11), (12, 4)\}$.

c) $z = 100 - x - y$ vaut 75, 78, 81, 84 (multiples de 3, ce qui est cohérent avec le prix des poussins). Si l'on veut au moins un animal de chaque sorte : $(4, 18, 78), (8, 11, 81), (12, 4, 84)$ (contrôle : $20 + 54 + 26 = 100$ ✓) ; sans cette exigence, il faut ajouter $(0, 25, 75)$.

3. a) Si $8x - 11y = 5$, alors $8x = 5 + 11y \equiv 5 [11]$. Tableau des restes modulo 11 :

x	0	1	2	3	4	5	6	7	8	9	10
$8x \text{ modulo } 11$	0	8	5	2	10	7	4	1	9	6	3

Donc $x \equiv 2 [11]$.

b) *Analyse.* $x = 2 + 11k$ ($k \in \mathbb{Z}$), puis $11y = 8x - 5 = 11 + 88k$, d'où $y = 1 + 8k$. *Synthèse.* $8(2 + 11k) - 11(1 + 8k) = 16 - 11 = 5$ ✓. $S = \{(2 + 11k, 1 + 8k), k \in \mathbb{Z}\}$.

4. $12(x+3) = 12x + 36 \equiv 12x [18]$: le reste de $12x$ ne dépend que du reste de x modulo 3, et vaut 0, 12, 6 pour $x \equiv 0, 1, 2 [3]$. Ainsi $12x \equiv b [18]$ a des solutions $\iff b \equiv 0, 6 \text{ ou } 12 [18] \iff 6 \mid b$. $12x \equiv 6 [18] \iff x \equiv 2 [3]$ ($12 \times 2 = 24 \equiv 6$ ✓).

■ Corrigé de l'exercice 59

1. a) Le volume passe de xyz à $(x+1)(y+1)(z+1)$: la condition s'écrit $(x+1)(y+1)(z+1) = 2xyz$; en divisant par $xyz > 0$: $\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right)\left(1 + \frac{1}{z}\right) = 2$.

b) *Encadrement.* $x \leq y \leq z$ donne $\frac{1}{z} \leq \frac{1}{y} \leq \frac{1}{x}$, donc chaque facteur est $\leq 1 + \frac{1}{x}$ et $2 \leq \left(1 + \frac{1}{x}\right)^3$. Si $x \geq 4$: $\left(1 + \frac{1}{x}\right)^3 \leq \left(\frac{5}{4}\right)^3 = \frac{125}{64} < 2$, contradiction. Si $x = 1$: $\left(1 + \frac{1}{y}\right)\left(1 + \frac{1}{z}\right) = 1$, impossible car chaque facteur est > 1 . Donc $x \in \{2, 3\}$ (et $\left(\frac{4}{3}\right)^3 = \frac{64}{27} \geq 2$ ✓).

c) *Cas $x = 2$:* $3(y+1)(z+1) = 4yz \iff yz - 3y - 3z = 3 \iff (y-3)(z-3) = 12$. Si $y \in \{2, 3\}$, le membre de gauche est ≤ 0 : donc $1 \leq y-3 \leq z-3$ et $(y-3, z-3) \in \{(1, 12), (2, 6), (3, 4)\}$, soit $(y, z) \in \{(4, 15), (5, 9), (6, 7)\}$.

Cas $x = 3$: $2(y+1)(z+1) = 3yz \iff yz - 2y - 2z = 2 \iff (y-2)(z-2) = 6$, avec $1 \leq y-2 \leq z-2$: $(y, z) \in \{(3, 8), (4, 5)\}$.

Cinq pavés : $2 \times 4 \times 15, 2 \times 5 \times 9, 2 \times 6 \times 7, 3 \times 3 \times 8, 3 \times 4 \times 5$ (par exemple $4 \times 5 \times 6 = 120 = 2 \times 60$ ✓).

2. Supposons $x \leq y \leq z$. Alors $w! > z!$ (car $x! + y! > 0$), donc $w > z$, soit $w \geq z+1$ et $w! \geq (z+1)! = (z+1)z!$. D'autre part $x! + y! + z! \leq 3z!$. Donc $(z+1)z! \leq 3z!$, soit $z \leq 2$. Alors $x!, y!, z!$ valent 1 ou 2, et la somme $w!$ est comprise entre 3 et 6 : c'est $6 = 3!$, atteint seulement pour $x! = y! = z! = 2$. $(x, y, z, w) = (2, 2, 2, 3)$ ($2 + 2 + 2 = 6 = 3!$).

■ Corrigé de l'exercice 60

1. a) Si $x = 0$, $-4^y = 0$: impossible ; si $y = 0$, $5^x = 2$: impossible. Donc $x \geq 1$ et $y \geq 1$.

b) Modulo 3 : $5 \equiv -1$ et $4 \equiv 1$, donc $(-1)^x \equiv 1 + 1 = 2 \equiv -1 [3]$. Si x était pair, on aurait $1 \equiv -1 [3]$: faux. Donc x est impair.

c) $5^x - 1 = (5 - 1)(1 + 5 + \dots + 5^{x-1}) = 4S$; S est une somme de x nombres impairs, avec x impair, donc S est impair. L'équation donne $4^y = 4S$, soit $S = 4^{y-1}$: une puissance de 4 impaire vaut 1, donc $y = 1$ et $S = 1$, ce qui impose $x = 1$. Réciproquement $5 - 4 = 1$: $(x, y) = (1, 1)$.

2. a) $(2n^2 + n)^2 = 4n^4 + 4n^3 + n^2$ et $4P(n) = 4n^4 + 4n^3 + 4n^2 + 4n + 4$: la différence vaut $3n^2 + 4n + 4$. De même $(2n^2 + n + 1)^2 = 4n^4 + 4n^3 + 5n^2 + 2n + 1$, et $4P(n) - (2n^2 + n + 1)^2 = -n^2 + 2n + 3 = -(n-3)(n+1)$.
- b) $3n^2 + 4n + 4$ a un discriminant $16 - 48 < 0$: il est toujours > 0 . Si $n < -1$ ou $n > 3$, $(n-3)(n+1) > 0$. Avec $M = 2n^2 + n = n(2n+1) \geq 0$ (deux facteurs de même signe, ou $n = 0$) : $M^2 < 4P(n) < (M+1)^2$.
- c) Si $P(n) = m^2$ ($m \in \mathbb{N}$), alors $4P(n) = (2m)^2$; pour $n < -1$ ou $n > 3$, b) donne $M < 2m < M+1$: impossible entre deux entiers consécutifs. Il reste $n \in \{-1, 0, 1, 2, 3\}$, où $P(n) = 1, 1, 5, 31, 121$: $P(n)$ est un carré $\iff n \in \{-1, 0, 3\}$ ($P(3) = 121 = 11^2$).

35

Corrigés : défis de concours

■ Corrigé de l'exercice 61

- $2^n = x^2 + 615 \geq 615 > 512 = 2^9$, donc $n \geq 10$. Alors 2^n est pair et 615 impair : $x^2 = 2^n - 615$ est impair, donc x est impair (le carré d'un pair est pair).
- $615 = 3 \times 205 \equiv 0 [3]$ et $2 \equiv -1 [3]$: l'équation donne $x^2 \equiv (-1)^n [3]$. Un carré est congru à 0 ou 1 modulo 3, et $(-1)^n$ à 1 ou 2 : nécessairement $(-1)^n \equiv 1$, donc n est pair (et $3 \nmid x$).
- $2^n - x^2 = (2^m)^2 - x^2 = (2^m - x)(2^m + x) = 615 = 3 \times 5 \times 41$. Posons $u = 2^m - x$, $v = 2^m + x$: $v > 0$ et $uv > 0$ donnent $u > 0$; $x \geq 1$ donne $u < v$; enfin $u + v = 2^{m+1}$.

(u, v)	$(1, 615)$	$(3, 205)$	$(5, 123)$	$(15, 41)$
$u + v$	$616 = 8 \times 77$	$208 = 16 \times 13$	$128 = 2^7$	$56 = 8 \times 7$

Seul $u + v = 128$ est une puissance de 2 : $m + 1 = 7$, $m = 6$, $n = 12$ et $x = \frac{v-u}{2} = 59$. $(x, n) = (59, 12)$ ($59^2 + 615 = 3481 + 615 = 4096 = 2^{12}$ ✓).

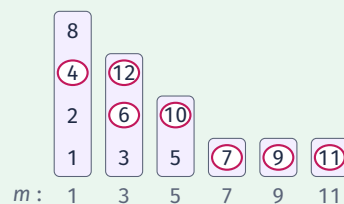
- Même méthode : $2^n \geq 63 > 32$ donne $n \geq 6$, puis x impair ; $63 \equiv 0 [3]$ donne $n = 2m$ pair, et $(2^m - x)(2^m + x) = 63 = 3^2 \times 7$. Les couples (u, v) sont $(1, 63)$, $(3, 21)$, $(7, 9)$, de sommes $64 = 2^6$, 24 et $16 = 2^4$: $m = 5$, $x = 31$ ou $m = 3$, $x = 1$. $(x, n) \in \{(31, 10), (1, 6)\}$ ($961 + 63 = 1024$, $1 + 63 = 64$ ✓).

■ Corrigé de l'exercice 62

- a) *Principe des tiroirs*. Les n tiroirs $\{2j-1, 2j\}$ ($1 \leq j \leq n$) recouvrent $\{1, \dots, 2n\}$. Par l'absurde, si chaque tiroir contenait au plus un élément de A , A aurait au plus n éléments : contradiction. Un tiroir contient donc deux éléments de A , qui sont $2j-1$ et $2j$: **deux entiers consécutifs**.
b) Pour tout k , un diviseur commun de k et $k+1$ divise $(k+1) - k = 1$: $k \wedge (k+1) = 1$. Les deux entiers consécutifs trouvés sont premiers entre eux.
- a) *Existence*. Soit α l'exposant de 2 dans la décomposition de k ($\alpha = 0$ si k est impair) : $m = \frac{k}{2^\alpha}$ est un entier impair. *Unicité*. Si $2^\alpha m = 2^\beta m'$ avec m, m' impairs et, par exemple, $\alpha < \beta$, alors $m = 2^{\beta-\alpha} m'$ serait pair : absurde. Donc $\alpha = \beta$, puis $m = m'$.
b) Si $k \leq 2n$, sa partie impaire $m \leq k$ est un impair de $\{1, 3, \dots, 2n-1\}$: n valeurs possibles (les tiroirs), pour $n+1$ éléments de A . Deux éléments distincts $a = 2^\alpha m$ et $b = 2^\beta m$ ont donc la même partie impaire ; $a \neq b$ impose $\alpha \neq \beta$, disons $\alpha < \beta$: $b = 2^{\beta-\alpha} a$, donc $a \mid b$ et le quotient est une puissance de 2.

3. $A = \{2, 4, \dots, 2n\}$ a n éléments, tous pairs : deux d'entre eux ont un PGCD ≥ 2 . $A = \{n+1, n+2, \dots, 2n\}$ a n éléments : si $a < b$ sont dans A et $a \mid b$, alors $b \geq 2a \geq 2n+2$, absurde. **Les deux résultats sont donc optimaux.**

4. Ici $n = 1013$: parmi 1014 entiers distincts de $\{1, \dots, 2026\}$, il y en a toujours **deux qui sont premiers entre eux** (deux consécutifs) et **deux dont l'un divise l'autre**, le quotient étant une puissance de 2. Avec 1013 entiers, ce n'est plus garanti : les pairs $2, 4, \dots, 2026$, ou les entiers $1014, \dots, 2026$, sont des contre-exemples.



Question 2b pour $n = 6$: les entiers de 1 à 12 rangés en 6 tiroirs selon leur partie impaire m . Sept entiers choisis (cerclés) ne tiennent pas dans 6 tiroirs : ici 6 et $12 = 2 \times 6$.

■ Corrigé de l'exercice 63

- $P(a)$: « $3^a \geq 2a + 1$ ». *Initialisation.* $3^0 = 1 = 2 \times 0 + 1$. *Hérédité.* Supposons $P(a)$ vraie pour un $a \geq 0$: $3^{a+1} = 3 \times 3^a \geq 6a + 3 \geq 2a + 3 = 2(a+1) + 1$. *Conclusion.* $P(a)$ est vraie pour tout $a \in \mathbb{N}$. Il y a égalité pour $a = 0$ et $a = 1$ ($3 = 3$) ; si $a \geq 1$, $6a + 3 > 2a + 3$, donc $3^{a+1} > 2(a+1) + 1$: **l'inégalité est stricte pour $a \geq 2$** . Enfin, si $p \geq 5$ et $a \geq 1$: $p^a \geq 5^a > 3^a \geq 2a + 1$.
- a) $n = d(n)^2$ est un carré : si $d(n) = p_1^{a_1} \dots p_k^{a_k}$, alors $n = p_1^{2a_1} \dots p_k^{2a_k}$ (et $k \geq 1$ car $n \geq 2$). Donc $d(n) = (2a_1 + 1) \dots (2a_k + 1)$ est un produit d'impairs : $d(n)$ **est impair**, et $n = d(n)^2$ aussi. Ainsi 2 n'est pas l'un des p_i : $p_i \geq 3$.
b) n et $d(n)$ étant positifs : $n = d(n)^2 \iff \sqrt{n} = d(n) \iff p_1^{a_1} \dots p_k^{a_k} = (2a_1 + 1) \dots (2a_k + 1)$.
- D'après 1, chaque facteur vérifie $p_i^{a_i} \geq 2a_i + 1 > 0$ ($p_i \geq 3$, $a_i \geq 1$), avec égalité **seulement** si $p_i = 3$ et $a_i = 1$. Le produit des membres de gauche est donc $\geq$ celui des membres de droite, avec égalité si et seulement si chaque facteur réalise l'égalité ; comme les p_i sont distincts, cela impose $k = 1$, $p_1 = 3$, $a_1 = 1$, soit $n = 3^2 = 9$. Réciproquement $d(9) = 3$ et $3^2 = 9$ ✓, et $d(1) = 1$: $n \in \{1, 9\}$.

■ Corrigé de l'exercice 64

- 5 divise pqr et 5 est premier : d'après le lemme d'Euclide, il divise l'un des facteurs, qui, étant premier, vaut 5. Notons $s \leq t$ les deux autres : $5st = 5(5 + s + t)$, soit $st - s - t + 1 = 6$, c'est-à-dire $(s-1)(t-1) = 6$ avec $1 \leq s-1 \leq t-1$: $(s, t) \in \{(2, 7), (3, 4)\}$, et 4 n'est pas premier. $(p, q, r) = (2, 5, 7)$ ($2 \times 5 \times 7 = 70 = 5 \times 14$ ✓).
- Disjonction des cas.* Si p et q sont impairs, $p^q + q^p$ est pair et > 2 : non premier. Si $p = q = 2$: 8, non premier. Donc l'un vaut 2, disons $q = 2$, et p est un premier impair : $N = p^2 + 2^p$. Si $p = 3$: $N = 9 + 8 = 17$, premier. Si $p \geq 5$: $3 \nmid p$, donc $p^2 \equiv 1 [3]$; p est impair, donc $2^p \equiv (-1)^p = -1 [3]$; ainsi $3 \mid N$ avec $N > 3$: non premier. $\{p, q\} = \{2, 3\}$, et $2^3 + 3^2 = 17$.
- $p = 2$: $15 = 3 \times 5$ a 4 diviseurs ; $p = 3$: $20 = 2^2 \times 5$ a $3 \times 2 = 6$ diviseurs. Si $p \geq 5$: p est impair, donc $p^2 \equiv 1 [8]$ et $p^2 + 11 \equiv 12 \equiv 4 [8]$: l'exposant de 2 dans $p^2 + 11$ vaut exactement 2 ; et $p^2 \equiv 1 [3]$ donne $3 \mid p^2 + 11$. Ainsi $p^2 + 11 = 2^2 \times 3^\beta \times M$, avec $\beta \geq 1$ et M premier avec 6, et $d(p^2 + 11) = 3(\beta + 1)d(M) \geq 6$, avec égalité seulement si $\beta = 1$ et $M = 1$, c'est-à-dire $p^2 + 11 = 12$, $p = 1$: absurde. $p = 3$.

■ **Corrigé de l'exercice 65**

1. $1 + 1 + 1 = 3 = 3 \times 1 \times 1$ ✓. Si (a, b) est solution de (E_k) : $(a - b)^2 \geq 0$ donne $a^2 + b^2 \geq 2ab$, donc $kab = a^2 + b^2 + 1 > 2ab$ et $k > 2$: $k \geq 3$. Soit $\delta = a \wedge b$: δ^2 divise a^2 , b^2 et kab , donc divise $kab - a^2 - b^2 = 1$: $a \wedge b = 1$.

2. a) $aa' = kab - a^2 = b^2 + 1$ (d'après (E_k)). Donc $a' = \frac{b^2+1}{a} > 0$, et $a' = kb - a \in \mathbb{Z}$: $a' \in \mathbb{N}^*$. Puis

$$a'^2 + b^2 + 1 - ka'b = a'(a' - kb) + b^2 + 1 = -aa' + b^2 + 1 = 0 : (a', b) \text{ est solution.}$$

b) Par l'absurde, supposons $a \geq b + 1$. Alors $a' = \frac{b^2+1}{a} \leq \frac{b^2+1}{b+1} \leq b$ (car $b^2 + 1 \leq b^2 + b$). Par symétrie de (E_k) , le couple (b, a') est solution, avec $b \geq a'$ et $b + a' < b + a$: cela contredit la minimalité de $a + b$. Donc $a = b$.

c) Alors $2a^2 + 1 = ka^2$, soit $(k - 2)a^2 = 1$: $a^2 \mid 1$, donc $a = b = 1$ et $k = 3$. **Conclusion** : (E_k) a des solutions si et seulement si $k = 3$, c'est-à-dire que si $\frac{a^2+b^2+1}{ab}$ est entier, il vaut 3.

3. Posons $c = 3b - a$: $c^2 + b^2 + 1 - 3cb = c(c - 3b) + b^2 + 1 = -ac + b^2 + 1 = a^2 + b^2 + 1 - 3ab = 0$: (c, b) , donc (b, c) , est solution ; et $a \leq b$ donne $c \geq 2b > b$. En partant de $(1, 1)$:

$$(1, 1) \rightarrow (1, 2) \rightarrow (2, 5) \rightarrow (5, 13) \rightarrow (13, 34) \rightarrow (34, 89) \rightarrow \dots$$

(par exemple $13^2 + 34^2 + 1 = 1326 = 3 \times 13 \times 34$ ✓). La seconde coordonnée augmente strictement : ces solutions sont deux à deux distinctes, et (E_3) a une infinité de solutions.

■ **Corrigé de l'exercice 66**

1. Le nombre de zéros finaux de $n!$ est le plus grand entier t tel que $10^t = 2^t 5^t$ divise $n!$, c'est-à-dire le plus petit des exposants de 2 et de 5 dans $n!$. Or $2^j \leq 5^j$ donne $E\left(\frac{n}{2^j}\right) \geq E\left(\frac{n}{5^j}\right)$ pour tout j : l'exposant de 2 est le plus grand, et $Z(n) = E\left(\frac{n}{5}\right) + E\left(\frac{n}{25}\right) + \dots$.

2. a) $E\left(\frac{N}{m}\right)$ est le nombre de multiples de m dans $\{1, \dots, N\}$ (ce sont $m, 2m, \dots, qm$ avec $qm \leq N < (q+1)m$). Les entiers $5q+1, \dots, 5q+r$ ne sont pas multiples de 5 : les multiples de 5^j ($j \geq 1$) de $\{1, \dots, 5q+r\}$ sont ceux de $\{1, \dots, 5q\}$, de la forme $5i$ avec $1 \leq i \leq q$ et $5^{j-1} \mid i$: il y en a $E\left(\frac{q}{5^{j-1}}\right)$. En sommant sur $j \geq 1$: $Z(5q+r) = q + E\left(\frac{q}{5}\right) + E\left(\frac{q}{25}\right) + \dots = q + Z(q)$.

b) $(n+1)! = (n+1) \times n!$, donc l'exposant de 5 ne peut qu'augmenter : Z est croissante. D'après a), Z est constante sur chaque bloc $\{5q, \dots, 5q+4\}$ ($q \geq 1$), et $Z(5q+5) = q+1 + Z(q+1) \geq q+1 + Z(q) > Z(5q+4)$: chaque valeur non nulle est prise **exactement 5 fois** (la valeur 0 est prise pour $n = 1, \dots, 4$).

c) Avec $5^j \leq n < 5^{j+1}$ ($Z(n) = 0 < \frac{n}{4}$ si $n < 5$) : $Z(n) \leq \frac{n}{5} + \dots + \frac{n}{5^j} = \frac{n}{5} \times \frac{1-5^{-j}}{1-\frac{1}{5}} = \frac{n}{4} (1 - 5^{-j}) < \frac{n}{4}$.

3. a) $Z(8120) = 1624 + 324 + 64 + 12 + 2 = 2026$, $Z(8119) = 1623 + 324 + 64 + 12 + 2 = 2025$, $Z(8125) = 1625 + 325 + 65 + 13 + 2 = 2030$ ($8125 = 13 \times 5^4$).

b) D'après 2c, $Z(n) = 2026$ impose $n > 4 \times 2026 = 8104$: c'est ce qui guide le calcul de a). Z étant croissante, avec $Z(8119) = 2025$ et $Z(8125) = 2030$, et constante sur le bloc $\{8120, \dots, 8124\}$: $Z(n) = 2026 \iff 8120 \leq n \leq 8124$.

c) Si $n \leq 8124$, $Z(n) \leq Z(8124) = 2026$; si $n \geq 8125$, $Z(n) \geq 2030$. **Aucune factorielle ne se termine par 2027, 2028 ou 2029 zéros** : Z « saute » de 4 en 8125, car $5^4 \mid 8125$.

Corrigé du test d'entrée

Barème : 1 point par réponse juste et justifiée, $\frac{1}{2}$ point si une seule des deux parties est juste. Reporte tes points bloc par bloc dans la case score de la page 4.

Bloc 1 · Arithmétique

- ① (a) 1, 3, 5, 15, 25, 75 ;
(b) 15. $75 = 3 \times 5^2$; de
 $208 = 13 \times 16$ à
 $390 = 13 \times 30$.
- ② (a) 2, 3, 4, 9 ;
(b) $a \in \{0, 3, 6, 9\}$. Somme
des chiffres 18,
 $48 = 4 \times 12$; $12 + a$
multiple de 3.
- ③ (a) 197 ; (b) $2^2 \times 7^2 \times 11$.
 $187 = 11 \times 17$,
 $203 = 7 \times 29$; 2, 3, 5, 7, 11,
13 ne divisent pas 197
($17^2 > 197$).
- ④ (a) 30 et 900 ; (b) à 8 h 20.
 $150 = 2 \times 3 \times 5^2$,
 $180 = 2^2 \times 3^2 \times 5$; PPCM de
16 et 20 : 80 min.

Bloc 2 · Raisonnements

- ⑤ $n = 2k$:
 $5n^2 + 3n = 2(10k^2 + 3k)$;
 $n = 2k + 1$:
 $5n^2 + 3n = 2(10k^2 + 13k + 4)$.
- ⑥ (a) Si $a \leq 6$ et $b \leq 6$, alors
 $ab \leq 36$. (b) On multiplie
ces deux inégalités entre
nombres positifs.
- ⑦ (a) $100 = 3(2a + 5b)$:
absurde ; $1 + 0 + 0 = 1$, non
multiple de 3.
(b) $99 = 4 \times 6 + 5 \times 15$.
- ⑧ (a) $u_0 = 2 \times 3^0 - 1$;
(b) $u_4 = 161 = 7 \times 23$.
Hérédité :
 $3(2 \times 3^n - 1) + 2 = 2 \times 3^{n+1} - 1$;
 u_4 n'est pas premier.

Bloc 3 · Calcul et puissances

- ⑨ (a) $2^4 \times 3 = 48$; (b) 7×2^n .
 $2^{5+6-7} \times 3^{5-4}$; $2^n(2^3 - 2 + 1)$.
- ⑩ (a) $(x - 3y)(x + 3y)$;
(b) 47×53 .
 $50^2 - 3^2 = (50 - 3)(50 + 3)$;
47 et 53 sont premiers.
- ⑪ (a) $a = 2$, $b = 1$, $c = 5$;
(b) $n = 3$. Quotient
 $= 2n + 1 + \frac{5}{n+2}$; $n + 2$ divise
5 et $n + 2 \geq 2$, d'où
 $n + 2 = 5$.
- ⑫ (a) 6 et 11 ; (b) $[-6, 4]$: 11
entiers. $X^2 - 17X + 66 = 0$,
 $\Delta = 25$; $(x + 6)(x - 4) \leq 0$:
de -6 à 4.

Ton orientation

les renvois sont cliquables dans le PDF

1. Selon ton score total : par où commencer, quels exercices faire en priorité.

0 à 5
bases à revoir

Commence par tes erreurs (ce corrigé sert de rappel), puis le cours pas à pas, sections 1 à 3 d'abord, puis 6 et 7. **En priorité** : le niveau 1, **exercices 1 à 8**, p. 23 ; puis **exercice 31**, p. 29 et **exercice 43**, p. 32. Refais le test dans une semaine.

6 à 9
bon départ

Commence par le cours complet (sections 1 à 11), puis les pièges de la section 13. **En priorité** : le niveau 2, **exercices 9 à 16**, p. 24 ; puis les thèmes B et D, **exercices 37 à 42**, p. 30 et **49 à 54**, p. 34.

10 à 12
cap concours

Commence par le cours (sections 1 à 11 en lecture rapide), puis les sections 12 à 14. **En priorité** : le niveau 3, **exercices 17 à 23**, p. 26 ; les thèmes C et E, **exercices 43 à 48**, p. 32 et **55 à 60**, p. 36 ; puis le niveau 4, **exercices 24 à 30**, p. 27, et le thème F, **61 à 66**, p. 37.

2. Selon ton bloc le plus faible (2 points sur 4 ou moins) : fais d'abord sa case, puis ta ligne ci-dessus.

Bloc 1 · Arithmétique

Relis : les sections 1 et 6 à 9 du cours.
Fais : **exercice 5**, p. 24,
exercice 6, p. 24, **exercice 44**,
p. 32 et **exercice 49**, p. 34.

Bloc 2 · Raisonnements

Relis : les sections 2, 3, 6 et 11 du cours.
Fais : **exercice 3**, p. 23,
exercice 12, p. 25, **exercice 34**,
p. 30 et **exercice 57**, p. 36.

Bloc 3 · Calcul et puissances

Relis : les sections 1, 5, 11 et 14 du cours.
Fais : **exercice 9**, p. 24,
exercice 14, p. 25, **exercice 38**,
p. 31 et **exercice 56**, p. 36.

Mon bilan sur le chapitre

Partie B · Le parcours en 4 niveaux

Niveau	Exercices	Réussis seul(e)	À refaire
Niveau 1 · Bases ★	1 à 8	/ 8	
Niveau 2 · Bac ★★	9 à 16	/ 8	
Niveau 3 · Approfondissement ★★★	17 à 23	/ 7	
Niveau 4 · Concours ★★★★	24 à 30	/ 7	

Partie C · La banque d'exercices

Thème	Exercices	Réussis seul(e)	À refaire
Thème A · Divisibilité et division euclidienne	31 à 36	/ 6	
Thème B · Congruences	37 à 42	/ 6	
Thème C · Nombres premiers	43 à 48	/ 6	
Thème D · PGCD et PPCM	49 à 54	/ 6	
Thème E · Équations en nombres entiers	55 à 60	/ 6	
Thème F · Défis de concours	61 à 66	/ 6	

Conseil : refais dans une semaine les exercices ratés, sans regarder le corrigé.

Prochain chapitre : Calcul vectoriel dans l'espace

Maths Olympiad