

Chapitre 8

Arithmétique

dans $\mathbb{Z}$

Du niveau de base au niveau concours

*À connaître par cœur*Bézout : $a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$ Fermat : p premier,
 $p \nmid a \Rightarrow a^{p-1} \equiv 1 [p]$ *Défi de concours*Chiffre des unités de 7^{7^7} : ?

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

crible d'Ératosthène : les 19 nombres premiers jusqu'à 70

★★★★ Niveau 4 · Concours

★★★ Niveau 3 · Approfondissement

★★ Niveau 2 · Bac

★ Niveau 1 · Bases

Cours complet

Méthodes et pièges

66 exercices corrigés

Formulaire

Sommaire

1	Divisibilité dans $\mathbb{Z}$	6
2	Division euclidienne	7
3	Congruences modulo n	8
4	Applications des congruences	9
4.1	Numération en base b	9
4.2	Critères de divisibilité	10
4.3	Chiffre des unités, restes de grandes puissances	10
5	PGCD et algorithme d'Euclide	11
6	Le théorème de Bézout	12
7	Le théorème de Gauss et le PPCM	13
7.1	Le PPCM	14
8	Nombres premiers	14
9	Le petit théorème de Fermat	16
10	Équations $ax + by = c$ et systèmes	18
10.1	Systèmes de congruences	19
11	Pour aller plus loin	19
11.1	L'ensemble $\mathbb{Z}/n\mathbb{Z}$	19
11.2	Nombres de Mersenne et de Fermat	20
12	Les pièges classiques	20
13	Les astuces des concours	21
14	L'essentiel du chapitre en une page	23
15	Niveau 1 · Bases	24
16	Niveau 2 · Bac	25
17	Niveau 3 · Approfondissement	27
18	Niveau 4 · Concours	28

19	Division euclidienne	30
20	Congruences et restes	32
21	PGCD et théorème de Bézout	34
22	Gauss et nombres premiers	36
23	Équations diophantiennes	38
24	Défis de concours	40
25	Corrigés du niveau 1	42
26	Corrigés du niveau 2	44
27	Corrigés du niveau 3	47
28	Corrigés du niveau 4	50
29	Corrigés : division euclidienne	52
30	Corrigés : congruences et restes	56
31	Corrigés : PGCD et Bézout	59
32	Corrigés : Gauss et nombres premiers	63
33	Corrigés : équations diophantiennes	66
34	Corrigés : défis de concours	69

Comment utiliser ce livret**Les 4 niveaux d'exercices****Niveau 1 · Bases ★**

les automatismes indispensables.

Niveau 2 · Bac ★★

le niveau de l'examen national.

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.

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 (Division euclidienne, Congruences et restes, PGCD et théorème de Bézout, Gauss et nombres premiers, Équations diophantiennes, 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.

La carte du chapitre



À la fin du chapitre, je sais...

- | | |
|--|---|
| ☐ utiliser les combinaisons linéaires $bu + cv$; | ☐ trouver des coefficients de Bézout ; |
| ☐ effectuer une division euclidienne ; | ☐ appliquer le théorème de Gauss, calculer un PPCM ; |
| ☐ raisonner par disjonction de cas ; | ☐ décomposer en facteurs premiers, compter les diviseurs ; |
| ☐ calculer avec les congruences ; | ☐ utiliser le petit théorème de Fermat ; |
| ☐ dresser et lire un tableau de restes ; | ☐ résoudre $ax + by = c$ dans $\mathbb{Z}^2$; |
| ☐ trouver le reste d'une grande puissance ; | ☐ résoudre un système de congruences. |
| ☐ utiliser les critères, la base b ; | |
| ☐ calculer un PGCD par l'algorithme d'Euclide ; | |

Partie A • Le cours

Définitions, théorèmes, méthodes, pièges et astuces de concours

1 Divisibilité dans $\mathbb{Z}$

Définition

Soit a et b deux entiers relatifs. On dit que a **divise** b , et l'on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$; on dit aussi que a est un **diviseur** de b , ou que b est un **multiple** de a . On note $D(b)$ l'ensemble des diviseurs de b , et $a\mathbb{Z} = \{ka, k \in \mathbb{Z}\}$ l'ensemble des multiples de a . Sinon, on note $a \nmid b$.

Exemples : $-6 \mid 42$; $D(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$; tout entier divise 0, mais 0 ne divise que 0 ; 1 et -1 divisent tout entier. Un entier est **pair** s'il est multiple de 2, **impair** sinon.

Théorème

Soit a, b, c, d des entiers relatifs et $n \in \mathbb{N}$.

1. $a \mid a$; si $a \mid b$ et $b \mid c$, alors $a \mid c$ (**transitivité**) ; $a \mid b \iff -a \mid b \iff a \mid -b \iff |a| \mid |b|$.
2. **Combinaisons linéaires** : si $a \mid b$ et $a \mid c$, alors $a \mid bu + cv$ pour tous $u, v \in \mathbb{Z}$ (en particulier $a \mid b + c$ et $a \mid b - c$).
3. Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$: un entier non nul n'a qu'un nombre **fini** de diviseurs.
4. Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$, c'est-à-dire $b = \pm a$.
5. Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$; en particulier $a \mid b \implies ac \mid bc$ et $a \mid b \implies a^n \mid b^n$.

Démonstration. 1. $a = 1 \times a$; si $b = ka$ et $c = k'a$, alors $c = (k'k)a$ avec $k'k \in \mathbb{Z}$; enfin $b = ka \iff b = (-k)(-a) \iff -b = (-k)a$. 2. Si $b = ka$ et $c = k'a$, alors $bu + cv = (ku + k'v)a$ avec $ku + k'v \in \mathbb{Z}$. 3. Si $b = ka$ et $b \neq 0$, alors $k \neq 0$, donc $|k| \geq 1$ et $|b| = |k| |a| \geq |a|$. 4. Si $b = 0$, alors $b \mid a$ impose $a = 0$; sinon $a \neq 0$ et le point 3 donne $|a| \leq |b|$ et $|b| \leq |a|$. 5. $b = ka$ et $d = k'a$ donnent $bd = (kk')ac$; puis on prend $c = d$, et l'on raisonne par récurrence sur n . $\square$

Méthode : montrer que a divise une expression, trouver les n tels que $A(n) \mid B(n)$

- Écrire l'expression sous la forme ka avec k **entier**, ou utiliser une récurrence.
- Si $d \mid A$ et $d \mid B$, alors d divise toute combinaison $uA + vB$: on choisit u et v (entiers) pour **éliminer** n .

Exemple : trois raisonnements types

- **Les entiers n tels que $n + 2 \mid 3n + 11$.** Comme $n + 2 \mid 3(n + 2)$, si $n + 2 \mid 3n + 11$, alors $n + 2$ divise $(3n + 11) - 3(n + 2) = 5$. Réciproquement, si $n + 2 \mid 5$, alors $n + 2 \mid 5 + 3(n + 2) = 3n + 11$. Donc $n + 2 \in D(5) = \{-5, -1, 1, 5\}$, soit $n \in \{-7, -3, -1, 3\}$.
- **L'équation $x^2 - y^2 = 15$ dans $\mathbb{N}^2$.** Elle s'écrit $(x - y)(x + y) = 15$ avec $x + y \geq 0$, donc $x + y > 0$, puis $x - y > 0$ et $x - y \leq x + y$: $(x - y, x + y) \in \{(1, 15), (3, 5)\}$, d'où $(x, y) = (8, 7)$ ou $(4, 1)$, qui conviennent.
- **Par récurrence : $7 \mid 3^{2n+1} + 2^{n+2}$ pour tout $n \in \mathbb{N}$.** Soit $u_n = 3^{2n+1} + 2^{n+2}$: $u_0 = 3 + 4 = 7$, et

$$u_{n+1} = 9 \times 3^{2n+1} + 2 \times 2^{n+2} = 9u_n - 7 \times 2^{n+2}.$$

Si $7 \mid u_n$, alors 7 divise la combinaison $9u_n - 7 \times 2^{n+2} = u_{n+1}$: la propriété est héréditaire. (Preuve plus rapide en section 3.)

2**Division euclidienne****Théorème (division euclidienne)**

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

q est le **quotient** et r le **reste** de la division euclidienne de a par b . On a $q = E\left(\frac{a}{b}\right)$, et $b \mid a \iff r = 0$.

Démonstration. Existence. L'ensemble $A = \{a - bk, k \in \mathbb{Z}\} \cap \mathbb{N}$ est une partie **non vide** de $\mathbb{N}$: pour $k = -|a|$, $a - bk = a + b|a| \geq a + |a| \geq 0$. Elle admet donc un plus petit élément $r = a - bq$, et $r \geq 0$. Si l'on avait $r \geq b$, alors $r - b = a - b(q + 1)$ serait un élément de A strictement plus petit que r : c'est absurde, donc $0 \leq r < b$.

Unicité. Si $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$, alors $b \mid q - q' = |r' - r| < b$, donc $|q - q'| < 1$: $q = q'$ (entiers), puis $r = r'$. Enfin, $0 \leq a - bq < b \iff q \leq \frac{a}{b} < q + 1 \iff q = E\left(\frac{a}{b}\right)$. $\square$

Remarque. Pour $b \in \mathbb{Z}^*$ négatif, on divise par $|b|$: il existe un unique (q, r) tel que $a = bq + r$ et $0 \leq r < |b|$. Le reste est **toujours positif** : $2026 = 13 \times 155 + 11$, mais $-47 = 6 \times (-8) + 1$ (et non $6 \times (-7) - 5$) ; on retrouve $-8 = E\left(-\frac{47}{6}\right)$.

Méthode : raisonner par disjonction de cas

La division par b montre que tout entier s'écrit de **l'une** des formes $bk, bk + 1, \dots, bk + (b - 1)$ ($k \in \mathbb{Z}$). Pour prouver une propriété pour tout n , on traite chacun de ces b cas (la section 3 le fait plus vite avec les congruences).

Exemple : tout entier est de la forme $2k$ (pair) ou $2k + 1$ (impair) ; deux entiers consécutifs n'ont pas la même parité, donc $n(n + 1)$ **est toujours pair**.

Le carré d'un impair

Si n est impair, alors $8 \mid n^2 - 1$.

Démonstration. $n = 2k + 1$, donc $n^2 - 1 = 4k^2 + 4k = 4k(k + 1)$, et $k(k + 1)$ est pair : $k(k + 1) = 2m$, d'où $n^2 - 1 = 8m$. $\square$

Exemple : deux problèmes de division

- **6 divise $P = n(n + 1)(2n + 1)$ pour tout $n \in \mathbb{Z}$.** $n(n + 1)$ est pair, donc $2 \mid P$. Pour 3 : si $n = 3k$, $3 \mid n$; si $n = 3k + 1$, $2n + 1 = 3(2k + 1)$; si $n = 3k + 2$, $n + 1 = 3(k + 1)$: dans tous les cas $3 \mid P$, soit $P = 3m$. Alors 2 divise $P - 2m = m$, donc $6 \mid P$. (Ainsi $\frac{n(n+1)(2n+1)}{6} = 1^2 + 2^2 + \dots + n^2$ est bien un entier.)
- **Un entier naturel n a le même quotient q dans ses divisions par 23 et par 25, avec les restes 17 et 3.** Alors $n = 23q + 17 = 25q + 3$, donc $2q = 14$, $q = 7$ et $n = 178$. Réciproquement, $178 = 23 \times 7 + 17$ avec $0 \leq 17 < 23$, et $178 = 25 \times 7 + 3$ avec $0 \leq 3 < 25$: ce sont bien les divisions euclidiennes.

3 Congruences modulo n **Définition**

Soit $n \in \mathbb{N}^*$. Deux entiers a et b sont **congrus modulo n** si $n \mid a - b$; on note $a \equiv b [n]$. Ainsi $a \equiv b [n] \iff \exists k \in \mathbb{Z}, a = b + kn$.

Théorème

Soit $n \in \mathbb{N}^*$ et a, b, c, d des entiers.

1. $a \equiv b [n] \iff a$ et b ont le **même reste** dans la division euclidienne par n . Si r est le reste de a , alors $a \equiv r [n]$, et r est l'**unique** entier de $\{0, 1, \dots, n - 1\}$ congru à a ; $a \equiv 0 [n] \iff n \mid a$.
2. **Relation d'équivalence** : $a \equiv a [n]$; si $a \equiv b [n]$, alors $b \equiv a [n]$; si $a \equiv b [n]$ et $b \equiv c [n]$, alors $a \equiv c [n]$.
3. **Compatibilité** : si $a \equiv b [n]$ et $c \equiv d [n]$, alors

$$a + c \equiv b + d [n], \quad a - c \equiv b - d [n], \quad ac \equiv bd [n], \quad a^k \equiv b^k [n] \quad (k \in \mathbb{N}).$$

Démonstration. 1. Écrivons $a = nq + r$ et $b = nq' + r'$ avec $0 \leq r, r' < n$. Alors $a - b = n(q - q') + (r - r')$. Si $r = r'$, alors $n \mid a - b$. Réciproquement, si $n \mid a - b$, alors n divise la combinaison $(a - b) - n(q - q') = r - r'$, avec $|r - r'| < n$: d'après la section 1 (point 3), $r - r' = 0$. 2. Découle de 1 (« avoir le même reste »). 3. $(a + c) - (b + d) = (a - b) + (c - d)$ et $ac - bd = a(c - d) + d(a - b)$ sont des combinaisons linéaires de $a - b$ et de $c - d$, donc des multiples de n ; enfin, par récurrence sur k : $a^{k+1} = a^k \times a \equiv a^k \times b = b^k \times b = b^{k+1} [n]$. $\square$

Méthode : calculer modulo n

Dans une somme, un produit ou une puissance, on peut **remplacer chaque nombre par un nombre qui lui est congru** : son reste, ou un représentant plus commode comme $-1, -2, \dots$ Si

P est un polynôme à coefficients entiers et $a \equiv b [n]$, alors $P(a) \equiv P(b) [n]$.

Exemple : $3^{2n+1} + 2^{n+2} = 3 \times 9^n + 4 \times 2^n \equiv 3 \times 2^n + 4 \times 2^n = 7 \times 2^n \equiv 0 [7]$, car $9 \equiv 2 [7]$: on retrouve, en une ligne, le résultat de la section 1.

Méthode : le tableau de restes

Pour étudier une expression en x modulo n , il suffit de connaître le reste de x : on remplit un tableau avec les n restes possibles $0, 1, \dots, n-1$ (ou $0, \pm 1, \pm 2, \dots$, plus rapide grâce à la symétrie $(-x)^2 = x^2$).

Exemple : les carrés modulo 7

$x \equiv$	0	1	2	3	4	5	6
$x^2 \equiv$	0	1	4	2	2	4	1

(modulo 7)

Un carré est donc congru à 0, 1, 2 ou 4 modulo 7, jamais à 3, 5 ou 6.

• $x^2 \equiv 2 [7] \iff x \equiv 3$ ou $x \equiv 4 [7]$ (en vert).

• L'équation $x^2 = 7y + 5$ n'a pas de solution dans $\mathbb{Z}^2$.

Conséquence : $7 \mid x^2 + y^2 \iff (7 \mid x \text{ et } 7 \mid y)$. En effet, la somme de deux éléments de $\{0, 1, 2, 4\}$ n'est congrue à 0 modulo 7 que pour $0 + 0$ ($1 + 6, 2 + 5, 4 + 3$ sont exclus, car 3, 5, 6 ne sont pas des carrés modulo 7). Donc $x^2 \equiv y^2 \equiv 0$, soit $x \equiv y \equiv 0 [7]$ (colonne rouge). La réciproque est claire.

Attention, piège !

On **ne divise pas** une congruence : $2 \times 3 \equiv 2 \times 8 [10]$, et pourtant $3 \not\equiv 8 [10]$. La simplification par k est permise lorsque k et n sont premiers entre eux (théorème de Gauss, section 7).

4

Applications des congruences

4.1 Numération en base b

Théorème

Soit $b \geq 2$ un entier. Tout entier $N \in \mathbb{N}^*$ s'écrit de façon **unique** sous la forme

$$N = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0, \quad a_i \in \{0, 1, \dots, b-1\}, \quad a_k \neq 0;$$

on note $N = \overline{a_k a_{k-1} \dots a_1 a_0}^{(b)}$: ce sont les **chiffres** de N en base b .

Démonstration (récurrence forte sur N). Si $N < b$, on écrit $N = a_0$. Si $N \geq b$, la division euclidienne donne $N = bq + a_0$ avec $0 \leq a_0 < b$ et $1 \leq q < N$; par hypothèse de récurrence, $q = \overline{a_k \dots a_1}^{(b)}$, donc $N = bq + a_0 = \overline{a_k \dots a_1 a_0}^{(b)}$. Unicité : si $N = \overline{a_k \dots a_0}^{(b)}$, alors $N = b(a_k b^{k-1} + \dots + a_1) + a_0$ avec $0 \leq a_0 < b$: a_0 est le **reste** et $\overline{a_k \dots a_1}^{(b)}$ le **quotient** de N par b , uniques ; on conclut par récurrence. $\square$

Exemple : divisions successives : les restes, lus de bas en haut, sont les chiffres

- $2026 = 5 \times 405 + 1$, $405 = 5 \times 81 + 0$, $81 = 5 \times 16 + 1$, $16 = 5 \times 3 + 1$, $3 = 5 \times 0 + 3$: $2026 = \overline{31101}^{(5)}$ (contrôle : $3 \times 625 + 125 + 25 + 1 = 2026$).
- En base 2 : $2026 = 1024 + 512 + 256 + 128 + 64 + 32 + 8 + 2 = \overline{11111101010}^{(2)}$.
- Dans l'autre sens : $\overline{3021}^{(4)} = 3 \times 4^3 + 0 \times 4^2 + 2 \times 4 + 1 = 201$.

4.2 Critères de divisibilité**Théorème (en base 10, $N = \overline{a_k \dots a_1 a_0}$)**

- $10 \equiv 1 [9]$: $N \equiv a_0 + a_1 + \dots + a_k [9]$, donc aussi modulo 3 (**somme des chiffres**).
- $10 \equiv -1 [11]$: $N \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k [11]$ (**somme alternée**, en partant des unités).
- $4 \mid 100$ et $8 \mid 1000$: $N \equiv \overline{a_1 a_0} [4]$ et $N \equiv \overline{a_2 a_1 a_0} [8]$ (deux, trois derniers chiffres).
- $1001 = 7 \times 11 \times 13$, donc $1000 \equiv -1 [7]$: si $N = B_0 + 1000B_1 + 1000^2B_2 + \dots$ (tranches de trois chiffres), alors $N \equiv B_0 - B_1 + B_2 - \dots [7]$ (et de même modulo 11 et 13).
- Si $N = 10m + u$ (u chiffre des unités) : $7 \mid N \iff 7 \mid m - 2u$.

Démonstration. Par compatibilité, $10^i \equiv 1^i = 1 [9]$, $10^i \equiv (-1)^i [11]$ et $1000^i \equiv (-1)^i [7]$; on remplace dans $N = \sum a_i 10^i$. Puis $N = 100 \overline{a_k \dots a_2} + \overline{a_1 a_0}$ avec $4 \mid 100$ (idem avec $8 \mid 1000$). Enfin $N = 10(m - 2u) + 21u$ et $m - 2u = 21m - 2N$: si 7 divise l'un des nombres $N, m - 2u$, il divise l'autre. $\square$

Exemple : $N = 917\,538\,264$

Somme des chiffres : 45, donc $9 \mid N$. Somme alternée : $4 - 6 + 2 - 8 + 3 - 5 + 7 - 1 + 9 = 5$, donc $N \not\equiv 5 [11]$. $64 = 4 \times 16$ et $264 = 8 \times 33$: $4 \mid N$ et $8 \mid N$. Tranches : $264 - 538 + 917 = 643 = 7 \times 91 + 6$, donc $N \equiv 6 [7]$.

4.3 Chiffre des unités, restes de grandes puissances**Méthode : reste de a^m modulo n**

On cherche un petit exposant k tel que $a^k \equiv 1$ (ou -1) $[n]$; on divise m par k : si $m = kq + s$, alors $a^m = (a^k)^q a^s \equiv a^s [n]$. Le **chiffre des unités** de $N \in \mathbb{N}$ est son reste modulo 10 ; ses deux derniers chiffres forment son reste modulo 100.

Exemple : trois calculs

- $3^4 = 81 \equiv 1 [10]$ et $2026 = 4 \times 506 + 2$: $3^{2026} = (3^4)^{506} \times 3^2 \equiv 9 [10]$: le chiffre des unités de 3^{2026} est 9.
- $7^4 = 2401 \equiv 1 [100]$: $7^{2026} = (7^4)^{506} \times 49 \equiv 49 [100]$: 7^{2026} se termine par 49.
- $5^2 = 25 \equiv -1 [13]$: $5^{2026} = (5^2)^{1013} \equiv (-1)^{1013} = -1 \equiv 12 [13]$: le reste est 12.

Exemple : pour quels $n \in \mathbb{N}$ a-t-on $7 \mid 2^n + 3^n$?

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

$2^3 = 8 \equiv 1 [7]$ et $3^3 = 27 \equiv -1 [7]$, donc $3^6 \equiv 1 [7]$: les restes de 2^n et de 3^n se répètent avec la **période** 6. On écrit $n = 6q + s$ et on lit le tableau :

$$7 \mid 2^n + 3^n \iff n \equiv 3 [6].$$

5

PGCD et algorithme d'Euclide

Définition

Soit a et b deux entiers **non tous deux nuls**. L'ensemble $D(a) \cap D(b)$ des diviseurs communs contient 1 et il est fini (ses éléments divisent celui des deux entiers qui n'est pas nul) : son plus grand élément est le **plus grand commun diviseur** de a et b , noté $\text{PGCD}(a, b)$ ou $a \wedge b$. On a $a \wedge b \geq 1$, $a \wedge b = b \wedge a = |a| \wedge |b|$, $a \wedge 0 = |a|$ ($a \neq 0$), et, si $b \neq 0$: $b \mid a \iff a \wedge b = |b|$.

Lemme d'Euclide (la clé de tout le chapitre)

Si $a = bq + r$ avec a, b, q, r entiers, alors a, b ont les **mêmes diviseurs communs** que b, r ; en particulier $a \wedge b = b \wedge r$.

Démonstration. Si $d \mid a$ et $d \mid b$, alors $d \mid a - bq = r$; si $d \mid b$ et $d \mid r$, alors $d \mid bq + r = a$. $\square$

Théorème (algorithme d'Euclide)

Soit a, b dans $\mathbb{N}^*$. On pose $r_0 = a$, $r_1 = b$, puis, tant que $r_k \neq 0$, on note r_{k+1} le reste de la division de r_{k-1} par r_k . Il existe un rang N tel que $r_N \neq 0$ et $r_{N+1} = 0$, et

$$a \wedge b = r_N \quad (\text{le dernier reste non nul}).$$

De plus, les diviseurs communs de a et b sont exactement les diviseurs de $a \wedge b$.

Démonstration. Tant qu'ils sont définis, les restes vérifient $0 \leq r_{k+1} < r_k$: une suite strictement décroissante d'entiers naturels ne peut pas avoir plus de $b + 1$ termes, donc on atteint un reste nul, $r_{N+1} = 0$. D'après le lemme, appliqué à chaque division $r_{k-1} = r_k q_k + r_{k+1}$, les couples (r_0, r_1) , (r_1, r_2) , ..., $(r_N, 0)$ ont tous les mêmes diviseurs communs : ce sont les diviseurs de r_N (puisque tout entier divise 0). Le plus grand d'entre eux est r_N . $\square$

Théorème (homogénéité)

Pour tous a, b non tous deux nuls et tout $k \in \mathbb{Z}^*$: $(ka) \wedge (kb) = |k| (a \wedge b)$.
En particulier, si $d = a \wedge b$, $a = da'$ et $b = db'$, alors $a' \wedge b' = 1$.

Démonstration. Les signes n'interviennent pas ; on suppose $a, b, k > 0$ (si a ou b est nul, c'est immédiat). En multipliant par k chaque division de l'algorithme : $kr_{i-1} = (kr_i)q_i + kr_{i+1}$ avec $0 \leq kr_{i+1} < kr_i$, ce sont exactement les divisions euclidiennes de l'algorithme pour (ka, kb) ; son dernier reste non nul est donc $kr_N = k(a \wedge b)$. Enfin $d = (da') \wedge (db') = d(a' \wedge b')$, donc $a' \wedge b' = 1$. $\square$

Exemple : $1547 \wedge 560$: l'algorithme présenté en tableau

dividende	diviseur	reste	quotient
1547	560	427	2
560	427	133	1
427	133	28	3
133	28	21	4
28	21	7	1
21	7	0	3

Chaque ligne est une division euclidienne :
 $1547 = 560 \times 2 + 427$, $560 = 427 \times 1 + 133$,
 $427 = 133 \times 3 + 28$, $133 = 28 \times 4 + 21$, $28 = 21 \times 1 + 7$, $21 = 7 \times 3 + 0$.

À chaque étape, le **diviseur devient dividende** et le **reste devient diviseur** (flèches).
 Le dernier reste non nul (encadré) est 7 :

$$1547 \wedge 560 = 7.$$

Exemple : le PGCD de deux expressions : $d_n = (3n + 4) \wedge (n + 3)$, $n \in \mathbb{N}$

$3n + 4 = 3(n + 3) - 5$, donc, par le lemme d'Euclide, $d_n = (n + 3) \wedge (-5) = (n + 3) \wedge 5$: d_n divise 5, donc $d_n \in \{1, 5\}$, et

$$d_n = 5 \iff 5 \mid n + 3 \iff n \equiv 2 [5] \quad (\text{par exemple } d_7 = 25 \wedge 10 = 5 \text{ et } d_8 = 28 \wedge 11 = 1).$$

6

Le théorème de Bézout**Définition**

Deux entiers a et b sont **premiers entre eux** si $a \wedge b = 1$, c'est-à-dire si leurs seuls diviseurs communs sont 1 et -1 . Par exemple, deux entiers consécutifs n et $n + 1$ sont premiers entre eux (un diviseur commun divise $(n + 1) - n = 1$).

Théorème (identité de Bézout)

Soit a et b deux entiers non tous deux nuls. Il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$. De plus, $a \wedge b$ est le plus petit entier strictement positif de la forme $au + bv$, et les entiers de la forme $au + bv$ sont exactement les multiples de $a \wedge b$.

Démonstration. L'ensemble $E = \{au + bv, (u, v) \in \mathbb{Z}^2\} \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ (il contient $a^2 + b^2 = a \times a + b \times b$) : il a un plus petit élément $d = au_0 + bv_0$. Divisons a par d : $a = dq + r$ avec $0 \leq r < d$, et $r = a - (au_0 + bv_0)q = a(1 - qu_0) + b(-qv_0)$. Si r était non nul, il serait dans E et strictement inférieur à d : absurde. Donc $r = 0$ et $d \mid a$; de même $d \mid b$, donc $d \leq a \wedge b$. Inversement, $a \wedge b$ divise a et b , donc la combinaison $au_0 + bv_0 = d$, et $a \wedge b \leq d$. Ainsi $d = a \wedge b$. Enfin $a \wedge b$ divise tout $au + bv$, et $k(a \wedge b) = a(ku_0) + b(kv_0)$. $\square$

Théorème de Bézout

$$a \wedge b = 1 \iff \text{il existe } (u, v) \in \mathbb{Z}^2 \text{ tel que } au + bv = 1.$$

Démonstration. Le sens direct est l'identité de Bézout. Réciproquement, si $au + bv = 1$, tout diviseur commun à a et b divise $au + bv = 1$: il vaut ± 1 , donc $a \wedge b = 1$. $\square$

Méthode : trouver des coefficients de Bézout : l'algorithme d'Euclide « remonté »

On part de l'avant-dernière division, qui donne le PGCD, et on remplace successivement chaque reste en remontant les divisions. Avec 1547 et 560 (section 5) :

$$7 = 28 - 21 = 28 - (133 - 4 \times 28) = 5 \times 28 - 133 = 5 \times (427 - 3 \times 133) - 133 = 5 \times 427 - 16 \times 133 \\ = 5 \times 427 - 16 \times (560 - 427) = 21 \times 427 - 16 \times 560 = 21 \times (1547 - 2 \times 560) - 16 \times 560,$$

soit $1547 \times 21 + 560 \times (-58) = 7$ (contrôle : $32\,487 - 32\,480 = 7$). Ces coefficients ne sont pas uniques : la section 10 les donne tous.

Exemple : montrer que deux expressions sont premières entre elles

Pour tout $n \in \mathbb{Z}$: $3(2n+1) - 2(3n+2) = -1$, soit $(2n+1) \times (-3) + (3n+2) \times 2 = 1$: d'après le théorème de Bézout, $(2n+1) \wedge (3n+2) = 1$.

Conséquences

Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$. Par récurrence : si $a \wedge b = 1$, alors $a^m \wedge b^n = 1$ pour tous $m, n \in \mathbb{N}$.

Démonstration. Avec $au+bv = 1$ et $au'+cw = 1$: $1 = (au+bv)(au'+cw) = a(uau'+ucw+bvu')+bc(vw)$, et l'on applique le théorème de Bézout. $\square$

7 Le théorème de Gauss et le PPCM**Théorème de Gauss**

Soit a, b, c des entiers. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration. Par Bézout, $au + bv = 1$, donc $c = acu + bcv$. Or $a \mid acu$ et $a \mid bc$, donc a divise la combinaison $acu + (bc)v = c$. $\square$

Corollaires

1. Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$. (Plus généralement, des diviseurs de n premiers entre eux deux à deux : leur produit divise n .)
2. **Simplification** : si $ka \equiv kb \pmod{n}$ et $k \wedge n = 1$, alors $a \equiv b \pmod{n}$.

Démonstration. 1. $n = ak$; $b \mid ak$ et $b \wedge a = 1$, donc $b \mid k$ (Gauss) : $k = bk'$ et $n = abk'$. 2. $n \mid k(a-b)$ et $n \wedge k = 1$, donc $n \mid a-b$ (Gauss). $\square$

Exemple : deux applications

- **L'équation** $15x = 22y$ dans $\mathbb{Z}^2$. $15 \mid 22y$ et $15 \wedge 22 = 1$, donc $15 \mid y$ (Gauss) : $y = 15k$, puis $15x = 22 \times 15k$, soit $x = 22k$. Réciproquement, $(22k, 15k)$ convient : $S = \{(22k, 15k), k \in \mathbb{Z}\}$.
- $6 \mid n^3 + 5n$ pour tout $n \in \mathbb{Z}$. $n^3 + 5n = (n-1)n(n+1) + 6n$. Parmi trois entiers consécutifs, l'un est pair et l'un est multiple de 3 (section 2) : 2 et 3 divisent $(n-1)n(n+1)$, et $2 \wedge 3 = 1$, donc $6 \mid (n-1)n(n+1)$ (corollaire 1), puis $6 \mid n^3 + 5n$.

7.1 Le PPCM

Définition

Soit a et b deux entiers non nuls. L'ensemble des multiples communs strictement positifs de a et b contient $|ab|$: son plus petit élément est le **plus petit commun multiple**, noté $\text{PPCM}(a, b)$ ou $a \vee b$.

Théorème

Soit a, b deux entiers non nuls.

1. Les multiples communs de a et b sont exactement les multiples de $a \vee b$.
2. $(a \wedge b) \times (a \vee b) = |ab|$; en particulier, si $a \wedge b = 1$, alors $a \vee b = |ab|$.

Démonstration. On peut supposer $a, b > 0$. Soit $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$ (section 5), et $m = da'b' = ab'$: c'est un multiple commun de a et b . Si $M = ak = bl$ est un multiple commun, alors $da'k = db'l$, donc $a'k = b'l$: $b' \mid a'k$ et $b' \wedge a' = 1$, donc $b' \mid k$ (Gauss). Ainsi $k = b'k'$ et $M = ab'k' = mk'$: les multiples communs sont les multiples de m , et le plus petit strictement positif est m . Donc $a \vee b = m$ et $(a \wedge b)(a \vee b) = d \times da'b' = ab$. $\square$

Exemple : calculs de PPCM

- $120 = 84 + 36$, $84 = 2 \times 36 + 12$, $36 = 3 \times 12$: $84 \wedge 120 = 12$, donc $84 \vee 120 = \frac{84 \times 120}{12} = 840$.
- **Les couples** $(a, b) \in \mathbb{N}^{*2}$ **tels que** $a \wedge b = 12$ **et** $a \vee b = 360$. On écrit $a = 12a'$, $b = 12b'$ avec $a' \wedge b' = 1$. Alors $ab = 12 \times 360$, soit $144 a'b' = 4320$ et $a'b' = 30$. Les couples (a', b') sont $(1, 30)$, $(2, 15)$, $(3, 10)$, $(5, 6)$ et leurs symétriques (tous formés d'entiers premiers entre eux). Réciproquement, ils conviennent : il y a 8 couples,

$(a, b) \in \{(12, 360), (24, 180), (36, 120), (60, 72)\}$ et les couples symétriques.

8

Nombres premiers

Définition

Un entier naturel p est **premier** s'il a exactement deux diviseurs positifs, 1 et p (donc $p \geq 2$). Un entier $n \geq 2$ non premier est dit **composé**. Les premiers nombres premiers sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29... (1 n'est pas premier ; 2 est le seul nombre premier pair).

Théorème

1. Tout entier $n \geq 2$ admet au moins un diviseur premier : son plus petit diviseur $p > 1$ est premier.
2. Si $n \geq 2$ est composé, son plus petit diviseur premier p vérifie $p^2 \leq n$. Donc, **si aucun nombre premier** $p \leq \sqrt{n}$ **ne divise** n , **alors** n **est premier** (critère d'arrêt).

Démonstration. 1. 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 $1 < d' < p$, et

d' diviserait n (transitivité) : cela contredit la minimalité de p . 2. $n = pm$ avec $m \neq 1$ (car $n \neq p$) ; m est un diviseur > 1 de n , donc $m \geq p$, et $n = pm \geq p^2$. $\square$

Exemples : $20^2 = 400 < 401 < 441 = 21^2$, et aucun des nombres premiers 2, 3, 5, 7, 11, 13, 17, 19 ne divise 401 : 401 est premier. En revanche, pour 391 ($19^2 < 391 < 20^2$), on trouve $391 = 17 \times 23$.

Théorème (Euclide)

Il existe une **infinité** de nombres premiers.

Démonstration. Supposons qu'il n'y en ait qu'un nombre fini, $p_1, \dots, p_k$, et posons $N = p_1 p_2 \dots p_k + 1 \geq 3$. D'après le théorème précédent, N a un diviseur premier, qui est l'un des p_i ; alors p_i divise $N - p_1 p_2 \dots p_k = 1$: c'est absurde. $\square$

Méthode : le crible d'Ératosthène

On écrit les entiers de 2 à 100. On garde 2 et on barre tous ses multiples ; le premier nombre non barré, 3, est premier : on le garde et on barre ses multiples ; puis on recommence avec 5, puis 7.

Comme $11^2 = 121 > 100$, on peut s'arrêter : un nombre composé $n \leq 100$ a un diviseur premier $p \leq \sqrt{n} \leq 10$, donc il a été barré.

Il reste les 25 **nombres premiers** inférieurs à 100 (en bleu). Chaque nombre composé est barré dans la couleur de son plus petit facteur premier : 2, 3, 5, 7.

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

Théorème (lemme d'Euclide)

Soit p un nombre premier et a, b des entiers.

1. Ou bien $p \mid a$, ou bien $p \wedge a = 1$; deux nombres premiers distincts sont premiers entre eux.
2. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$. Plus généralement, si p divise un produit $a_1 a_2 \dots a_k$, il divise l'un des facteurs ; si $p \mid a^n$, alors $p \mid a$; si p divise un produit de nombres premiers, il est égal à l'un d'eux.

Démonstration. 1. $p \wedge a$ est un diviseur positif de p : il vaut 1 ou p , et $p \wedge a = p \iff p \mid a$. 2. Si $p \nmid a$, alors $p \wedge a = 1$ et $p \mid ab$, donc $p \mid b$ (Gauss). On généralise par récurrence sur k , avec $a_1 \dots a_{k+1} = (a_1 \dots a_k) \times a_{k+1}$; enfin, si p divise un nombre premier q , alors $p = q$ (car $p \neq 1$). $\square$

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ est un produit de nombres premiers :

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

et cette **décomposition en facteurs premiers** est unique.

Démonstration. Existence, par récurrence forte : 2 est premier. Soit $n > 2$ tel que tout entier m avec $2 \leq m < n$ se décompose. Si n est premier, c'est fini ; sinon, $n = pm$ avec p premier (son

plus petit diviseur > 1) et $2 \leq m < n$, et la décomposition de m donne celle de n . *Unicité*, par récurrence forte : si $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ (facteurs premiers, éventuellement répétés), alors p_1 divise $q_1 \cdots q_s$, donc p_1 est l'un des q_j (lemme d'Euclide). En simplifiant par p_1 , on obtient deux décompositions de $\frac{n}{p_1} < n$, qui ont les mêmes facteurs par hypothèse de récurrence (si $\frac{n}{p_1} = 1$, alors $r = s = 1$). $\square$

Théorème (diviseurs, PGCD et PPCM)

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, les diviseurs positifs de n sont les entiers $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$; leur nombre est $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

Le PGCD de deux entiers est le produit des facteurs premiers **communs**, affectés du **plus petit** exposant ; le PPCM est le produit de **tous** leurs facteurs premiers, affectés du **plus grand** exposant.

Démonstration. Un tel entier divise $n : n = (p_1^{\beta_1} \cdots p_k^{\beta_k}) \times p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k - \beta_k}$. Réciproquement, si $n = dd'$, tout facteur premier de d divise n , donc c'est l'un des p_i (lemme d'Euclide) ; par unicité de la décomposition de $n = dd'$, l'exposant de p_i dans n est la somme de ses exposants dans d et dans d' , donc $\beta_i \leq \alpha_i$. Toujours par unicité, deux choix différents des exposants donnent deux diviseurs différents : il y a $\alpha_i + 1$ choix pour chaque β_i . Les formules du PGCD et du PPCM en découlent. $\square$

Exemple : 504 et 540

$504 = 2^3 \times 3^2 \times 7$ et $540 = 2^2 \times 3^3 \times 5$, donc $504 \wedge 540 = 2^2 \times 3^2 = 36$ et $504 \vee 540 = 2^3 \times 3^3 \times 5 \times 7 = 7560$ (contrôle : $36 \times 7560 = 272\,160 = 504 \times 540$). Le nombre 7560 a $(3 + 1)(3 + 1)(1 + 1)(1 + 1) = 64$ diviseurs positifs.

Remarque. Le nombre de diviseurs positifs de n est impair $\iff$ tous les α_i sont pairs $\iff n$ est un carré parfait. Et si $n \in \mathbb{N}$ n'est pas un carré parfait, $\sqrt{n}$ est irrationnel : si $\sqrt{n} = \frac{a}{b}$, alors $nb^2 = a^2$, et les exposants de a^2 et de b^2 sont pairs, donc ceux de n aussi.

9

Le petit théorème de Fermat

Lemme

Si p est premier et $1 \leq k \leq p - 1$, alors $p \mid \binom{p}{k}$.

Démonstration. $k \binom{p}{k} = k \frac{p!}{k!(p-k)!} = p \frac{(p-1)!}{(k-1)!(p-k)!} = p \binom{p-1}{k-1}$, donc $p \mid k \binom{p}{k}$. Comme $1 \leq k < p$, $p \nmid k$, donc $p \wedge k = 1$, et $p \mid \binom{p}{k}$ (Gauss). $\square$

Petit théorème de Fermat

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$:

$$a^p \equiv a \pmod{p}$$

et, si $p \nmid a$:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Démonstration. Pour $a \in \mathbb{N}$, par récurrence : $0^p \equiv 0 [p]$; si $a^p \equiv a [p]$, la formule du binôme et le lemme donnent

$$(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 \equiv a^p + 1 \equiv a + 1 [p].$$

Pour $a \in \mathbb{Z}$, soit $r \in \mathbb{N}$ son reste modulo p : $a^p \equiv r^p \equiv r \equiv a [p]$. Enfin, si $p \nmid a$: $p \mid a^p - a = a(a^{p-1} - 1)$ et $p \wedge a = 1$, donc $p \mid a^{p-1} - 1$ (Gauss). $\square$

Exemple : deux applications directes

- **Reste de 2^{2026} modulo 13.** 13 est premier et ne divise pas 2, donc $2^{12} \equiv 1 [13]$. Comme $2026 = 12 \times 168 + 10$, $2^{2026} \equiv 2^{10} = 1024 = 13 \times 78 + 10 [13]$: le reste est 10.
- $30 \mid n^5 - n$ **pour tout** $n \in \mathbb{Z}$. Fermat avec $p = 5$: $n^5 \equiv n [5]$; avec $p = 3$: $n^5 = n^3 \times n^2 \equiv n \times n^2 = n^3 \equiv n [3]$; enfin n^5 et n ont la même parité. Ainsi 2, 3 et 5, premiers entre eux deux à deux, divisent $n^5 - n$: leur produit 30 aussi (corollaire de Gauss).

Théorème (le plus petit exposant)

Soit p premier et a un entier non divisible par p . L'ensemble des $k \in \mathbb{N}^*$ tels que $a^k \equiv 1 [p]$ est non vide (il contient $p-1$) ; soit k_0 son plus petit élément. Alors, pour tout $m \in \mathbb{N}$:

$$a^m \equiv 1 [p] \iff k_0 \mid m \quad ; \text{ en particulier, } k_0 \mid p-1.$$

Les restes de a^m se répètent avec la période k_0 : si $m \equiv s [k_0]$, alors $a^m \equiv a^s [p]$.

Démonstration. Écrivons $m = k_0 q + s$ avec $0 \leq s < k_0$: $a^m = (a^{k_0})^q a^s \equiv a^s [p]$. Si $a^m \equiv 1$, alors $a^s \equiv 1$ avec $0 \leq s < k_0$: par minimalité de k_0 , $s = 0$, donc $k_0 \mid m$. Réciproquement, si $k_0 \mid m$, alors $a^m = (a^{k_0})^q \equiv 1$. Avec $m = p-1$ (Fermat), on obtient $k_0 \mid p-1$. $\square$

Méthode : trouver le plus petit exposant : on ne teste que les diviseurs de $p-1$

Modulo 11, les diviseurs de 10 sont 1, 2, 5, 10.

- $2^1 = 2$, $2^2 = 4$, $2^5 = 32 \equiv -1 [11]$: le plus petit exposant de 2 est 10, donc $11 \mid 2^n - 1 \iff 10 \mid n$.
- $3^5 = 243 = 11 \times 22 + 1$ et $3 \not\equiv 1 [11]$: le plus petit exposant de 3 est 5 ; comme $2026 \equiv 1 [5]$, $3^{2026} \equiv 3 [11]$.

Attention, piège !

La réciproque du théorème de Fermat est **fausse** : $341 = 11 \times 31$ n'est pas premier, et pourtant $2^{340} \equiv 1 [341]$, car $2^{10} = 1024 = 3 \times 341 + 1$, donc $2^{340} = (2^{10})^{34} \equiv 1 [341]$. Et l'hypothèse $p \nmid a$ est indispensable : $14^6 \equiv 0 [7]$.

10

Équations $ax + by = c$ et systèmes

Théorème

Soit a, b des entiers non nuls, $c \in \mathbb{Z}$ et $d = a \wedge b$; on écrit $a = da'$ et $b = db'$ (donc $a' \wedge b' = 1$).

1. L'équation (E) : $ax + by = c$ a des solutions dans $\mathbb{Z}^2 \iff d \mid c$.

2. Si $d \mid c$ et si (x_0, y_0) est une solution particulière, les solutions de (E) sont les couples

$$x = x_0 + b'k, \quad y = y_0 - a'k, \quad k \in \mathbb{Z}.$$

Démonstration. 1. Si $ax + by = c$, alors d divise cette combinaison de a et b . Réciproquement, si $c = dc'$, l'identité de Bézout $au + bv = d$ donne $a(uc') + b(vc') = c$. 2. Soit $(x, y) \in \mathbb{Z}^2$. En retranchant $ax_0 + by_0 = c$, puis en divisant par d :

$$ax + by = c \iff a(x - x_0) = -b(y - y_0) \iff a'(x - x_0) = -b'(y - y_0).$$

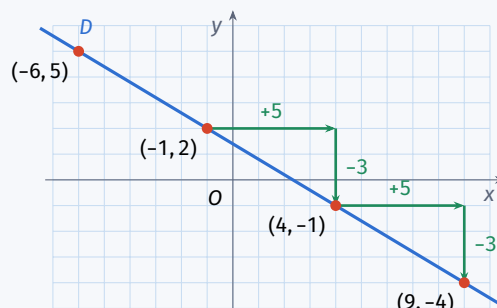
Si (x, y) est solution, $b' \mid a'(x - x_0)$ et $b' \wedge a' = 1$, donc $b' \mid x - x_0$ (Gauss) : $x = x_0 + b'k$; en reportant, $a'b'k = -b'(y - y_0)$, d'où $y = y_0 - a'k$ (car $b' \neq 0$). Réciproquement, ces couples vérifient $a'(b'k) = -b'(-a'k)$: ce sont des solutions. $\square$

Exemple : $3x + 5y = 7$: les points entiers d'une droite

$3 \wedge 5 = 1$ divise 7 ; solution évidente : $(4, -1)$. Alors $3(x - 4) = -5(y + 1)$: $5 \mid 3(x - 4)$ et $5 \wedge 3 = 1$, donc $x = 4 + 5k$, puis $y = -1 - 3k$: $S = \{(4 + 5k, -1 - 3k), k \in \mathbb{Z}\}$. Par Bézout, $3 \times 2 + 5 \times (-1) = 1$ donne la solution particulière $(14, -7)$ et l'écriture $\{(14 + 5k', -7 - 3k')\}$: c'est le **même ensemble** ($k' = k + 2$).

Les solutions sont les points à coordonnées entières de la droite $D : 3x + 5y = 7$; on passe de l'un au suivant par le vecteur $(5, -3) = (b', -a')$.

En revanche, $6x + 10y = 7$ n'a pas de solution : $6 \wedge 10 = 2 \nmid 7$.



Méthode : résoudre $ax + by = c$ dans $\mathbb{Z}^2$

1. Calculer $d = a \wedge b$ (Euclide) ; si $d \nmid c$, il n'y a **aucune** solution ; sinon, **diviser** l'équation par d .
2. Trouver une solution particulière (x_0, y_0) : « évidente », ou par Bézout (multiplier $a'u + b'v = 1$ par $c' = \frac{c}{d}$).
3. Retrancher, appliquer le théorème de Gauss, et **vérifier** que les couples obtenus conviennent.

Exemple : une résolution complète : $221x - 91y = 26$

- $221 = 91 \times 2 + 39$, $91 = 39 \times 2 + 13$, $39 = 13 \times 3$: $221 \wedge 91 = 13$, et $13 \mid 26$. On divise par 13 : $17x - 7y = 2$.
- Bézout : $17 = 7 \times 2 + 3$ et $7 = 3 \times 2 + 1$, donc $1 = 7 - 2 \times 3 = 7 - 2(17 - 2 \times 7) = 5 \times 7 - 2 \times 17$,

soit $17 \times (-2) - 7 \times (-5) = 1$; en multipliant par 2 : $(x_0, y_0) = (-4, -10)$.

- $17x - 7y = 17x_0 - 7y_0 \iff 17(x+4) = 7(y+10)$. Donc $7 \mid 17(x+4)$ et $7 \wedge 17 = 1 : x = -4 + 7k$ (Gauss), puis $y = -10 + 17k$; réciproquement, ces couples conviennent. Avec $k = k' + 1$:

$S = \{(3+7k', 7+17k'), k' \in \mathbb{Z}\}$; les solutions telles que $0 \leq x \leq 30$ ont $x \in \{3, 10, 17, 24\}$.

10.1 Systèmes de congruences

Théorème

Soit $m, n \in \mathbb{N}^*$ **premiers entre eux**, $(u, v) \in \mathbb{Z}^2$ tel que $mu + nv = 1$, et $a, b \in \mathbb{Z}$. Les solutions du système $\begin{cases} x \equiv a [m] \\ x \equiv b [n] \end{cases}$ sont les entiers

$$x \equiv x_0 [mn], \quad \text{où} \quad x_0 = a nv + b mu.$$

Démonstration. $nv = 1 - mu \equiv 1 [m]$ et $mu \equiv 0 [m]$, donc $x_0 \equiv a [m]$; de même $x_0 \equiv b [n]$. Si x est solution, alors $m \mid x - x_0$ et $n \mid x - x_0$ avec $m \wedge n = 1$, donc $mn \mid x - x_0$ (corollaire de Gauss). Réciproquement, si $x \equiv x_0 [mn]$, alors $x \equiv x_0$ modulo m et modulo n . $\square$

Exemple : $x \equiv 4 [7]$ et $x \equiv 6 [11]$

$7 \times (-3) + 11 \times 2 = 1$, donc $x_0 = 4 \times 11 \times 2 + 6 \times 7 \times (-3) = 88 - 126 = -38$: les solutions sont les entiers $x \equiv -38 \equiv 39 [77]$. Autre méthode : $x = 4 + 7k$ avec $7k \equiv 2 [11]$; comme $8 \times 7 = 56 \equiv 1 [11]$, on multiplie par 8 : $k \equiv 16 \equiv 5 [11]$, d'où $x = 4 + 7(5 + 11j) = 39 + 77j$. Contrôle : $39 = 7 \times 5 + 4 = 11 \times 3 + 6$.

11

Pour aller plus loin

11.1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Définition

Soit $n \geq 2$. La **classe** de $a \in \mathbb{Z}$ modulo n est l'ensemble $\bar{a} = \{a + kn, k \in \mathbb{Z}\}$ des entiers congrus à a ; $\bar{a} = \bar{b} \iff a \equiv b [n]$. L'ensemble des classes est $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$: il a exactement n éléments (un par reste possible). On pose $\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \times \bar{b} = \overline{ab}$: d'après la compatibilité (section 3), le résultat ne dépend pas des représentants choisis, et l'on calcule avec les règles usuelles.

Théorème (classes inversibles)

Soit $n \geq 2$ et $a \in \mathbb{Z}$. $\bar{a}$ est **inversible** dans $\mathbb{Z}/n\mathbb{Z}$ (il existe $\bar{u}$ tel que $\bar{a} \times \bar{u} = \bar{1}$) $\iff a \wedge n = 1$. Si p est premier, toute classe non nulle de $\mathbb{Z}/p\mathbb{Z}$ est inversible (l'inverse de $\bar{a}$ est $\bar{a}^{p-2}$), et $\bar{a} \times \bar{b} = \bar{0} \Rightarrow (\bar{a} = \bar{0} \text{ ou } \bar{b} = \bar{0})$.

Démonstration. $\bar{a} \times \bar{u} = \bar{1} \iff au \equiv 1 [n] \iff \exists v \in \mathbb{Z}, au + nv = 1$: on applique le théorème de Bézout. Si p est premier et $p \nmid a$, alors $a \wedge p = 1$ et $a \times a^{p-2} = a^{p-1} \equiv 1 [p]$ (Fermat) ; enfin, si $\bar{a} \times \bar{b} = \bar{0}$

avec $\bar{a} \neq \bar{0}$, on multiplie par l'inverse de $\bar{a}$. □

Exemple : la table de multiplication de $\mathbb{Z}/6\mathbb{Z}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

- $\bar{2} \times \bar{3} = \bar{0}$, alors que $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$ (en rouge) : un produit peut être nul sans qu'aucun facteur ne le soit !
- La diagonale montre que l'équation $x^2 = x$ a **quatre** solutions dans $\mathbb{Z}/6\mathbb{Z}$: $\bar{0}, \bar{1}, \bar{3}, \bar{4}$.
- Seuls $\bar{1}$ et $\bar{5}$ ont un inverse ($\bar{5} \times \bar{5} = \bar{1}$, en vert) : ce sont bien les classes des entiers premiers avec 6.

Exemple : dans $\mathbb{Z}/20\mathbb{Z}$, $\bar{7} \times \bar{3} = \bar{21} = \bar{1}$, donc $\bar{7}x = \bar{9} \iff x = \bar{3} \times \bar{9} = \bar{27} = \bar{7} : 7x \equiv 9 [20] \iff x \equiv 7 [20]$. En revanche, $\bar{6}$ n'est pas inversible ($6 \wedge 20 = 2$), et $6x \equiv 3 [20]$ n'a aucune solution (2 diviserait 3). □

11.2 Nombres de Mersenne et de Fermat

Théorème

1. Si $M_n = 2^n - 1$ est premier ($n \geq 2$), alors n est premier.
2. Si $2^m + 1$ est premier ($m \geq 1$), alors m est une puissance de 2 : c'est un **nombre de Fermat** $F_k = 2^{2^k} + 1$.
3. Pour $k \geq 1$, $F_0 F_1 \cdots F_{k-1} = F_k - 2$: deux nombres de Fermat distincts sont premiers entre eux.

Démonstration. 1. Si $n = rs$ avec $1 < r < n$, alors $2^r - 1$ divise $(2^r)^s - 1 = M_n$ (astuce 2 de la section 13) et $1 < 2^r - 1 < M_n$. 2. Écrivons $m = 2^k q$ avec q impair. Si $q \geq 3$, avec $A = 2^{2^k} : A + 1$ divise $A^q + 1 = 2^m + 1$ (q impair) et $1 < A + 1 < 2^m + 1$: impossible. Donc $q = 1$. 3. Par récurrence : $F_0 = 3 = F_1 - 2$; si $F_0 \cdots F_{k-1} = F_k - 2$, alors $F_0 \cdots F_k = (F_k - 2)F_k = (2^{2^k} - 1)(2^{2^k} + 1) = 2^{2^{k+1}} - 1 = F_{k+1} - 2$. Si $j < k$ et si d divise F_j et F_k , alors d divise $F_k - F_0 \cdots F_{k-1} = 2$, et d est impair : $d = \pm 1$. □

Remarque. Les réciproques sont fausses : 11 est premier, mais $M_{11} = 2047 = 23 \times 89$; $F_0, \dots, F_4$ (3, 5, 17, 257, 65 537) sont premiers, mais $F_5 = 641 \times 6\,700\,417$ (Euler). Chaque F_k a un diviseur premier, et ces diviseurs sont distincts deux à deux (point 3) : c'est une nouvelle preuve de l'infinité des nombres premiers.

12

Les pièges classiques

× Faux	✓ Vrai
« $2a \equiv 2b [n] \Rightarrow a \equiv b [n]$ »	seulement si $2 \wedge n = 1$: $2 \times 3 \equiv 2 \times 8 [10]$, mais $3 \not\equiv 8 [10]$
« $a \mid bc$ et $a \nmid b \Rightarrow a \mid c$ »	il faut $a \wedge b = 1$ (Gauss) : $6 \mid 4 \times 3$, mais $6 \nmid 4$ et $6 \nmid 3$

« $a \mid n$ et $b \mid n \Rightarrow ab \mid n$ »	seulement si $a \wedge b = 1$: $4 \mid 12$ et $6 \mid 12$, mais $24 \nmid 12$
« le reste de -17 dans la division par 5 est -2 »	$-17 = 5 \times (-4) + 3$: le reste est 3 (il vérifie $0 \leq r < 5$)
« $au + bv = 2 \Rightarrow a \wedge b = 2$ »	seulement $a \wedge b \mid 2$: $3 \times 4 + 5 \times (-2) = 2$ et $3 \wedge 5 = 1$; la réciproque de Bézout ne vaut que pour 1
« $a^2 \equiv b^2 [n] \Rightarrow a \equiv \pm b [n]$ »	$1^2 \equiv 3^2 [8]$, mais $3 \not\equiv \pm 1 [8]$; c'est vrai si n est premier
« $ab \equiv 0 [n] \Rightarrow a \equiv 0$ ou $b \equiv 0 [n]$ »	$2 \times 3 \equiv 0 [6]$; c'est vrai si n est premier (lemme d'Euclide)
« $m \equiv s [n] \Rightarrow a^m \equiv a^s [n]$ »	les exposants se réduisent modulo la période (par exemple $p - 1$), pas modulo n : $4 \equiv 1 [3]$, mais $2^4 \equiv 1 \not\equiv 2^1 [3]$
« $a^{p-1} \equiv 1 [p]$ pour tout a »	il faut p premier et $p \nmid a$: $14^6 \equiv 0 [7]$
« $2^{n-1} \equiv 1 [n] \Rightarrow n$ premier »	$341 = 11 \times 31$ et pourtant $2^{340} \equiv 1 [341]$
« $4x + 6y = 10$: $x = 1 + 6k$, $y = 1 - 4k$ »	on divise d'abord par $4 \wedge 6 = 2$: $x = 1 + 3k$, $y = 1 - 2k$; sinon on perd la solution $(4, -1)$
« 1 est premier » ; « p premier $\Rightarrow 2^p - 1$ premier »	1 n'a qu'un seul diviseur positif ; $2^{11} - 1 = 2047 = 23 \times 89$
« pour tester si n est premier, on essaie les diviseurs jusqu'à $\frac{n}{2}$ »	les nombres premiers $p \leq \sqrt{n}$ suffisent : jusqu'à 19 pour 401

13

Les astuces des concours★ **Astuce de concours : carrés modulo 4 et 8, cubes modulo 9**

Pour tout $x \in \mathbb{Z}$: $x^2 \equiv 0$ ou $1 [4]$; $x^2 \equiv 0, 1$ ou $4 [8]$ ($x^2 \equiv 1 [8]$ si x est impair) ; $x^3 \equiv 0, 1$ ou $-1 [9]$ (si $x = 3k \pm 1$, alors $x^3 = 27k^3 \pm 27k^2 + 9k \pm 1$).

- $x^2 + y^2 = 2027$ n'a pas de solution : $2027 \equiv 3 [4]$, alors qu'une somme de deux carrés est congrue à $0, 1$ ou 2 modulo 4 .
- 2023 n'est pas la somme de trois carrés : $2023 \equiv 7 [8]$, et une somme de trois éléments de $\{0, 1, 4\}$ n'est jamais congrue à 7 modulo 8 .
- $x^3 + y^3 + z^3 = 2030$ n'a pas de solution : $2030 \equiv 5 [9]$, alors qu'une somme de trois cubes est congrue à $0, \pm 1, \pm 2$ ou ± 3 modulo 9 .

★ **Astuce de concours : $a - b$ divise $a^n - b^n$**

$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$ (ou : $a \equiv b [a - b]$, donc $a^n \equiv b^n$). Si n est impair, $a^n + b^n = a^n - (-b)^n$ est divisible par $a + b$.

Exemples : $7 = 8 - 1$ divise $8^{675} - 1 = 2^{2025} - 1$; $3 = 2 + 1$ divise $2^{2027} + 1$; pour un polynôme P à coefficients entiers, $m - n$ divise $P(m) - P(n)$.

★ **Astuce de concours :** $(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1$ ($a \geq 2, m, n \in \mathbb{N}^*$)

Si $m = nq + r$, alors $a^m - 1 = a^r(a^{nq} - 1) + (a^r - 1)$, et $a^n - 1$ divise $(a^n)^q - 1$ (astuce précédente) : $a^m - 1 = (a^n - 1)Q + (a^r - 1)$ avec Q entier. Par le lemme d'Euclide (section 5), $(a^m - 1) \wedge (a^n - 1) = (a^n - 1) \wedge (a^r - 1)$: les exposants suivent l'algorithme d'Euclide de (m, n) , qui aboutit à $(a^{m \wedge n} - 1) \wedge (a^0 - 1) = a^{m \wedge n} - 1$.

Exemple : $84 \wedge 60 = 12$, donc $(2^{84} - 1) \wedge (2^{60} - 1) = 2^{12} - 1 = 4095$.

★ **Astuce de concours :** la descente infinie

Pour montrer qu'une équation n'a pas de solution non nulle, on part d'une solution « minimale » et on en fabrique une plus petite. Exemple : $x^2 + y^2 = 3z^2$ n'a que la solution $(0, 0, 0)$ dans $\mathbb{Z}^3$. Sinon, il existe une solution avec $z \neq 0$ (si $z = 0$, alors $x = y = 0$) ; prenons-en une avec $|z| \geq 1$ minimal. Modulo 3, un carré vaut 0 ou 1, et $x^2 + y^2 \equiv 0 [3]$ impose $x \equiv y \equiv 0 [3]$. Avec $x = 3x'$ et $y = 3y'$: $3(x'^2 + y'^2) = z^2$, donc $3 \mid z^2$, puis $3 \mid z$ (lemme d'Euclide) ; avec $z = 3z'$: $x'^2 + y'^2 = 3z'^2$ et $0 < |z'| < |z|$: contradiction. (Le cercle $x^2 + y^2 = 3$ n'a donc aucun point à coordonnées rationnelles.)

★ **Astuce de concours :** encadrement et divisibilité

Un multiple non nul de d vérifie $|m| \geq |d|$, et il n'y a aucun carré strictement entre k^2 et $(k+1)^2$.

- **Les $n \in \mathbb{N}$ tels que $n^2 + 2 \mid n^3 + 5$.** $n^3 + 5 = n(n^2 + 2) - (2n - 5)$, donc $n^2 + 2 \mid 2n - 5$. Si $n \geq 3$, alors $0 < 2n - 5 < n^2 + 2$: impossible. On teste $n = 0, 1, 2$: $2 \nmid 5, 3 \nmid 6, 6 \nmid 13$. Réponse : $n = 1$.
- **Les $n \in \mathbb{N}$ tels que $n^2 + 5n + 1$ soit un carré.** Si $n \geq 4$: $(n+2)^2 = n^2 + 4n + 4 < n^2 + 5n + 1 < n^2 + 6n + 9 = (n+3)^2$ (la première inégalité équivaut à $n > 3$) : ce n'est pas un carré. Pour $n = 0, 1, 2, 3$, on obtient 1, 7, 15, 25. Réponse : $n \in \{0, 3\}$.

★ **Astuce de concours :** factoriser pour obtenir « produit = constante »

$xy = 2x + 3y \iff xy - 2x - 3y + 6 = 6 \iff (x-3)(y-2) = 6$. Dans $\mathbb{N}^{*2}$: $y-2 \geq -1$, et $y-2 = -1$ donnerait $x = -3$; donc $y-2 \geq 1$, puis $x-3 \geq 1$: $(x-3, y-2) \in \{(1, 6), (2, 3), (3, 2), (6, 1)\}$, soit $(x, y) \in \{(4, 8), (5, 5), (6, 4), (9, 3)\}$.

★ **Astuce de concours :** combien de zéros à la fin de $n!$? (formule de Legendre)

L'exposant du nombre premier p dans $n!$ vaut $\sum_{k \geq 1} E\left(\frac{n}{p^k}\right)$: parmi $1, 2, \dots, n$, il y a $E\left(\frac{n}{p^k}\right)$ multiples de p^k , et chaque entier m est ainsi compté autant de fois que p apparaît dans sa décomposition. Les zéros finaux de $n!$ correspondent aux facteurs $10 = 2 \times 5$, et il y a plus de facteurs 2 que de facteurs 5 : $2026!$ se termine par $405 + 81 + 16 + 3 = \boxed{505}$ zéros.

14

L'essentiel du chapitre en une page

Divisibilité

$$a \mid b \iff b = ka \ (k \in \mathbb{Z}) ; a \mid b \text{ et } b \mid c \Rightarrow a \mid c$$

$$a \mid b \text{ et } a \mid c \Rightarrow a \mid bu + cv \ (u, v \in \mathbb{Z})$$

$$a \mid b, b \neq 0 \Rightarrow |a| \leq |b| ; a \mid b, b \mid a \Rightarrow b = \pm a$$

Division euclidienne ($a \in \mathbb{Z}, b \in \mathbb{N}^*$)

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

$$\text{cas : } n = bk + r, \ 0 \leq r < b ; n \text{ impair} \Rightarrow 8 \mid n^2 - 1$$

Congruences ($n \in \mathbb{N}^*$)

$$a \equiv b [n] \iff n \mid a - b \iff \text{même reste}$$

compatibles avec +, -, × et les puissances

$$ka \equiv kb [n] \text{ et } k \wedge n = 1 \Rightarrow a \equiv b [n]$$

$$a^k \equiv 1 [n] \Rightarrow a^{kq+s} \equiv a^s [n] \text{ (grandes puissances)}$$

Critères et numération

3 et 9 : somme des chiffres ; 4 : deux derniers chiffres

11 : somme alternée ; 8 : trois derniers chiffres

$$1000 \equiv -1 [7] ; 7 \mid 10m + u \iff 7 \mid m - 2u$$

$$\overline{a_k \dots a_0}^{(b)} = \sum a_i b^i, \ 0 \leq a_i < b$$

PGCD $a \wedge b$ et algorithme d'Euclide

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

diviseurs communs = diviseurs de $a \wedge b$

$$(ka) \wedge (kb) = |k| (a \wedge b)$$

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

Bézout

$$au + bv = a \wedge b \ (u, v \in \mathbb{Z} : \text{Euclide « remonté »})$$

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$$

$$a \wedge b = 1 \text{ et } a \wedge c = 1 \Rightarrow a \wedge bc = 1$$

Gauss et PPCM $a \vee b$

$$a \mid bc \text{ et } a \wedge b = 1 \Rightarrow a \mid c$$

$$a \mid n, b \mid n \text{ et } a \wedge b = 1 \Rightarrow ab \mid n$$

multiples communs = multiples de $a \vee b$

$$(a \wedge b) \times (a \vee b) = |ab|$$

Nombres premiers

aucun premier $p \leq \sqrt{n}$ ne divise $n \Rightarrow n$ premier

il y a une infinité de nombres premiers (Euclide)

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b ; p \nmid a \iff p \wedge a = 1$$

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ (unique)} : (\alpha_1 + 1) \dots (\alpha_k + 1) \text{ diviseurs}$$

PGCD : exposants min ; PPCM : exposants max

Petit théorème de Fermat (p premier)

$$p \mid \binom{p}{k} \ (0 < k < p) ; a^p \equiv a [p]$$

$$p \nmid a \Rightarrow a^{p-1} \equiv 1 [p]$$

$$k_0 \text{ plus petit exposant : } a^m \equiv 1 [p] \iff k_0 \mid m$$

donc $k_0 \mid p - 1$ (on teste les diviseurs de $p - 1$)

Équation $ax + by = c$ ($d = a \wedge b, a = da', b = db'$)

solutions $\iff d \mid c$; on divise par d , puis

Gauss

$$x = x_0 + b'k, y = y_0 - a'k, k \in \mathbb{Z}$$

(les points entiers d'une droite)

Système ($m \wedge n = 1, mu + nv = 1$)

$$x \equiv a [m] \text{ et } x \equiv b [n] \iff x \equiv a nv + b mu [mn]$$

$\mathbb{Z}/n\mathbb{Z}$, Mersenne, Fermat

$$\overline{a} + \overline{b} = \overline{a + b} ; \overline{a} \times \overline{b} = \overline{ab}$$

$$\overline{a} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \iff a \wedge n = 1$$

$$2^n - 1 \text{ premier} \Rightarrow n \text{ premier}$$

$$2^m + 1 \text{ premier} \Rightarrow m \text{ est une puissance de } 2$$

Astuces

$$x^2 \equiv 0, 1 [4] ; x^2 \equiv 0, 1, 4 [8] ; x^3 \equiv 0, \pm 1 [9]$$

$$a - b \mid a^n - b^n ; a + b \mid a^n + b^n \ (n \text{ impair})$$

$$(a^m - 1) \wedge (a^n - 1) = a^{m \wedge n} - 1 ; \text{descente infinie}$$

$$d \mid m \neq 0 \Rightarrow |m| \geq |d| ; k^2 < N < (k+1)^2 : \text{non carré}$$

$$(x - \alpha)(y - \beta) = \text{cte} ; \text{zéros de } n! : \sum_k E\left(\frac{n}{5^k}\right)$$

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 : $a \wedge b$ (PGCD), $a \vee b$ (PPCM), $\overline{a_k \dots a_0}^{(b)} = a_k b^k + \dots + a_0$ (base b ; sans précision : base 10).

15 Niveau I • Bases

Exercice 1 Divisibilité dans $\mathbb{Z}$ ★

corrigé p. 42

- Déterminer les entiers $n \in \mathbb{Z}$ tels que $n^2 + 1$ divise $n + 3$ (si $n + 3 \neq 0$, comparer $n^2 + 1$ et $|n + 3|$).
- Déterminer les entiers naturels n tels que $n + 1$ divise $n^2 + 7$.
- Soient $a, b \in \mathbb{Z}$. Montrer que : $13 \mid 2a + 3b \iff 13 \mid 5a + b$.
- Déterminer les couples $(x, y) \in \mathbb{N}^2$ tels que $x^2 = y^2 + 2y + 13$.

Exercice 2 Division euclidienne ★

corrigé p. 42

- Effectuer la division euclidienne de 1000, puis de -1000 , par 31.
- Le reste de la division de $a \in \mathbb{Z}$ par 12 est 7. Quels sont les restes de a par 4 et par 6, et de a^2 par 24 ?
- Montrer que la somme des carrés de trois entiers consécutifs n'est jamais un carré (modulo 3).
- Même question pour la somme des carrés de deux entiers impairs (modulo 4).

Exercice 3 Premiers calculs de congruences ★

corrigé p. 42

- Déterminer le reste de la division de : a) 3^{2026} par 7 b) 5^{2027} par 11 c) 100^{100} par 13.
- Résoudre dans $\mathbb{Z}$: a) $7x \equiv 4 \pmod{9}$ b) $6x \equiv 4 \pmod{10}$ c) $x^2 + x \equiv 0 \pmod{12}$ (dresser un tableau de restes).

Exercice 4 Grandes puissances et derniers chiffres ★

corrigé p. 43

- Déterminer le chiffre des unités de 8^{2027} et celui de 2027^{2027} .
- Déterminer les deux derniers chiffres de 9^{2026} (on pourra calculer 9^5 modulo 100).
- Déterminer le reste de la division euclidienne de $S = 1 + 2 + 2^2 + \dots + 2^{2026}$ par 7.
- Montrer que, pour tout $n \in \mathbb{N}$, l'entier $4^{2n+1} + 3^{n+2}$ est divisible par 13.

Exercice 5 Critères de divisibilité et bases ★

corrigé p. 43

- Déterminer les chiffres a et b tels que le nombre $\overline{2a3b6}$ soit divisible par 88.
- a) Écrire 500 en base 3, puis en base 6. b) Écrire en base 10 : $\overline{4E1}^{(16)}$ ($A, \dots, F$ notent 10, ..., 15).
- Déterminer la base b telle que $\overline{253}^{(b)} = 2 \times \overline{125}^{(b)}$.

Exercice 6 PGCD, algorithme d'Euclide, PPCM ★

corrigé p. 43

1. Calculer $4389 \wedge 2717$ (algorithme d'Euclide) et $4389 \vee 2717$; simplifier $2717/4389$.
2. Montrer que, pour tout $n \in \mathbb{N}$, $(n^2 + n) \wedge (2n + 1) = 1$.
3. Déterminer les couples $(a, b) \in \mathbb{N}^2$ tels que $a \leq b$ et $a \vee b - a \wedge b = 35$.
4. Quel est le plus petit $n \in \mathbb{N}$ dont les restes par 2, 3, 4, 5, 6 sont respectivement 1, 2, 3, 4, 5 ?

Exercice 7 Bézout et Gauss ★

corrigé p. 44

1. Montrer que $2026 \wedge 315 = 1$ et trouver $(u, v) \in \mathbb{Z}^2$ tel que $2026u + 315v = 1$.
2. En déduire $w \in \mathbb{Z}$ tel que $315w \equiv 1 [2026]$, puis résoudre dans $\mathbb{Z}$: $315x \equiv 5 [2026]$.
3. Montrer que le produit de quatre entiers consécutifs est divisible par 24.

Exercice 8 Nombres premiers et diviseurs ★

corrigé p. 44

1. Les entiers 523 et 527 sont-ils premiers ?
2. Décomposer 2016 et 2025 en facteurs premiers ; en déduire $2016 \wedge 2025$, $2016 \vee 2025$, leurs nombres de diviseurs et le nombre de diviseurs pairs de 2016.
3. Déterminer les entiers naturels n tels que $n^2 - 8n + 15$ soit un nombre premier.
4. Montrer que les 2026 entiers consécutifs $2027!, 2027!+1, 2027!+2, 2027!+3, \dots, 2027!+2027$ sont tous composés.

16

Niveau 2 · Bac**Exercice 9** Type examen national (1) : Fermat ★★

corrigé p. 44

1. a) Montrer que 47 est premier. b) Soit $x \in \mathbb{Z}$ non divisible par 47 ; justifier que $x^{46} \equiv 1 [47]$.
2. Soit $x \in \mathbb{Z}$ tel que $x^{17} \equiv 3 [47]$. a) Montrer que 47 ne divise pas x . b) Vérifier que $17 \times 19 = 7 \times 46 + 1$, et en déduire que $x \equiv 3^{19} [47]$.
3. a) Vérifier que $3^5 \equiv 8 [47]$ et $3^{10} \equiv 17 [47]$, puis que $3^{19} \equiv 18 [47]$. b) Montrer que $18^{17} \equiv 3 [47]$ et résoudre dans $\mathbb{Z}$ l'équation $x^{17} \equiv 3 [47]$.
4. Déterminer le reste de la division euclidienne de 18^{2026} par 47.

Exercice 10 Type examen national (2) : $ax + by = c$ ★★

corrigé p. 45

On considère dans $\mathbb{Z}^2$ l'équation (E) : $391x - 255y = 34$.

1. Calculer $391 \wedge 255$ par l'algorithme d'Euclide ; en déduire que (E) a des solutions et qu'elle équivaut à (E') : $23x - 15y = 2$.
2. Vérifier que $23 \times 2 - 15 \times 3 = 1$; en déduire une solution particulière de (E'), puis résoudre (E).
3. Combien (E) a-t-elle de solutions (x, y) telles que $0 \leq x \leq 2026$?
4. Déterminer les solutions (x, y) de (E) telles que $x^2 + y^2 < 2026$, et interpréter graphiquement.

Exercice 11 Type examen national (3) : PGCD ★★

corrigé p. 45

Soit n un entier naturel, $n \geq 2$. On pose $a = n^3 + 4n^2 - 5n$ et $b = 3n^2 - 2n - 1$.

1. Factoriser a et b ; en déduire que $n - 1$ divise a et b .
2. On pose $\alpha = n(n + 5)$ et $\beta = 3n + 1$. a) Montrer que $n \wedge \beta = 1$, puis que $\alpha \wedge \beta = (n + 5) \wedge \beta$. b) Montrer que $(n + 5) \wedge \beta$ divise 14. c) Calculer $(n + 5) \wedge \beta$ selon le reste de n modulo 14.
3. En déduire $a \wedge b$ en fonction de n , puis calculer $a \wedge b$ pour $n = 2025$ et pour $n = 2027$.

Exercice 12 Type examen national (4) : système de congruences ★★

corrigé p. 46

On considère le système (S) : $x \equiv 9 [14]$ et $x \equiv 4 [17]$, d'inconnue $x \in \mathbb{Z}$.

1. a) Vérifier que $5 \times 17 - 6 \times 14 = 1$. b) En déduire que $x_0 = 9 \times 85 - 4 \times 84$ est une solution de (S), et calculer x_0 .
2. Montrer que : x est solution de (S) $\iff x \equiv 191 [238]$.
3. Un collectionneur a moins de 500 billes. Rangées par paquets de 14, il en reste 9 ; par 17, il en reste 4 ; par 5, il en reste 1. Combien a-t-il de billes ?

Exercice 13 Tableaux de restes et impossibilités ★★

corrigé p. 46

1. Tableau des restes de x^2 modulo 5 ; en déduire que $2x^2 + 5y^2 = 2026$ n'a pas de solution dans $\mathbb{Z}^2$.
2. Montrer que l'équation $x^2 - 3y^2 = 2026$ n'a pas de solution dans $\mathbb{Z}^2$ (parité, puis modulo 8).
3. Montrer que $n^2 + 3n + 5$ n'est jamais divisible par 121 ($n \in \mathbb{Z}$) ; on écrira $n^2 + 3n + 5 = (n+7)(n-4) + 33$.
4. Tableau des restes de x^3 modulo 7 ; en déduire que si 7 ne divise ni x , ni y , ni z , alors $7 \nmid x^3 + y^3 + z^3$.

Exercice 14 Numération en base b ★★

corrigé p. 46

Soient $b \geq 2$ un entier et $N = \overline{a_k \dots a_1 a_0}^{(b)}$.

1. Montrer que $N \equiv a_0 + a_1 + \dots + a_k [b - 1]$ et $N \equiv a_0 - a_1 + a_2 - \dots + (-1)^k a_k [b + 1]$.
2. Sans le convertir en base 10, dire si le nombre $\overline{62415}^{(7)}$ est divisible par 6 ; par 8.
3. Déterminer les chiffres x tels que $\overline{3x5x2}^{(9)}$ soit divisible par 8 ; par 10.
4. a) Pour quelles bases b l'entier 2026 a-t-il trois chiffres ? b) Résoudre $2026 = \overline{101}^{(b)}$.

Exercice 15 Petit théorème de Fermat : applications ★★

corrigé p. 46

1. Montrer que $3^{2026} + 5^{2026}$ est divisible par 17.
2. Soit $n \in \mathbb{Z}$. a) Si p est premier et $p-1 \mid 12$, montrer que $n^{13} \equiv n [p]$. b) En déduire $2730 \mid n^{13} - n$.
3. Soit p un nombre premier, $p \geq 7$. Montrer que p divise l'entier $\underbrace{11 \dots 1}_{p-1 \text{ chiffres}}$.
4. Soit p un nombre premier. Montrer que $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 [p]$.

Exercice 16 Une suite d'entiers et ses restes ★★

corrigé p. 47

On considère la suite (u_n) définie par $u_0 = 1$ et $u_{n+1} = 2u_n + 3$ pour tout $n \in \mathbb{N}$.

1. Montrer par récurrence que $u_n = 2^{n+2} - 3$ pour tout $n \in \mathbb{N}$, puis que $u_n \wedge u_{n+1} = 1$.
2. a) Déterminer les entiers n tels que $5 \mid u_n$, puis ceux tels que $13 \mid u_n$. b) Existe-t-il n tel que $65 \mid u_n$?
3. Déterminer le chiffre des unités de u_{2026} .

17

Niveau 3 · Approfondissement**Exercice 17** Diviseurs et couples d'entiers ★★★

corrigé p. 47

On note $d(n)$ le nombre de diviseurs positifs de n : $d(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$ (cours).

1. Sachant que 1013 est premier, déterminer le plus petit entier $n \geq 1$ tel que $d(n) = 2026$.
2. Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, montrer qu'il y a 2^k couples $(a, b) \in \mathbb{N}^{*2}$ tels que $ab = n$ et $a \wedge b = 1$.
3. Montrer qu'il y a $(2\alpha_1 + 1) \cdots (2\alpha_k + 1)$ couples $(a, b) \in \mathbb{N}^{*2}$ tels que $a \vee b = n$. Cas $n = 360$.

Exercice 18 Diviseurs premiers de $2^p - 1$ et de $n^4 + 1$ ★★★

corrigé p. 47

Rappel (cours) : si q est premier, $q \nmid a$ et k est le plus petit entier $k \geq 1$ tel que $a^k \equiv 1 [q]$, alors $a^m \equiv 1 [q] \iff k \mid m$, et $k \mid q - 1$.

1. Soient p un nombre premier impair et q un diviseur premier de $2^p - 1$. Montrer que $q \equiv 1 [2p]$.
2. En n'effectuant que deux divisions, montrer que $2^{13} - 1 = 8191$ est premier.
3. Soient $n \in \mathbb{N}^*$ et q un diviseur premier impair de $n^4 + 1$. Montrer que $n^8 \equiv 1 [q]$, puis que le plus petit $k \geq 1$ tel que $n^k \equiv 1 [q]$ est 8. En déduire que $q \equiv 1 [8]$.
4. Application : décomposer $10\,001 = 10^4 + 1$ en produit de facteurs premiers.

Exercice 19 Calculs dans $\mathbb{Z}/n\mathbb{Z}$ ★★★

corrigé p. 48

1. Dans $\mathbb{Z}/11\mathbb{Z}$: a) résoudre l'équation $4x + 7 = 2$; b) résoudre le système $3x + 5y = 1, 2x - y = 4$; c) résoudre l'équation $x^2 = 5$.
2. Dans $\mathbb{Z}/12\mathbb{Z}$: a) déterminer les éléments inversibles et leurs inverses ; b) résoudre $4x = 8$; c) montrer que $3x = 5$ n'a pas de solution ; d) résoudre $x^2 = 1$.
3. Soit p premier. Montrer que, dans $\mathbb{Z}/p\mathbb{Z}$: $x^2 = 1 \iff (x = 1 \text{ ou } x = -1)$. Comparer avec 2.d.

Exercice 20 Carrés modulo p ★★★

corrigé p. 48

Soit p un nombre premier impair.

1. Montrer que $x^2 \equiv y^2 [p] \iff (x \equiv y \text{ ou } x \equiv -y [p])$. En déduire que, parmi $1, 2, \dots, p - 1$, exactement $\frac{p-1}{2}$ restes sont des carrés modulo p (ceux de $1^2, \dots, \left(\frac{p-1}{2}\right)^2$). Les donner pour $p = 13$.
2. Soit $a \equiv x^2 [p]$ avec $p \nmid a$. Montrer que $a^{\frac{p-1}{2}} \equiv 1 [p]$. En déduire que, si $p \equiv 3 [4]$, -1 n'est pas un carré modulo p , et que 3 n'est pas un carré modulo 31.
3. Soit $m \in \mathbb{N}^*$. Montrer que tout diviseur premier q de $4m^2 + 1$ vérifie $q \equiv 1 [4]$. En déduire qu'il existe une infinité de nombres premiers de la forme $4k + 1$.

Exercice 21 Valuations p -adiques ★★★

corrigé p. 48

Pour p premier et $n \in \mathbb{Z}^*$, $v_p(n)$ est l'exposant de p dans la décomposition de $|n|$ (0 si $p \nmid n$).

1. Montrer que $v_p(ab) = v_p(a) + v_p(b)$, et que, pour $a, b \in \mathbb{N}^*$: $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout p .
2. Soient $a, b, n \in \mathbb{N}^*$. Montrer que si $a^n \mid b^n$, alors $a \mid b$. En déduire que $\sqrt[3]{2026}$ est irrationnel.
3. Si $ab = c^n$ et $a \wedge b = 1$ ($a, b, c, n \in \mathbb{N}^*$), montrer que a et b sont des puissances n -ièmes.
4. Soit $n \in \mathbb{N}^*$. Montrer que $n(n+1)$, puis $n(n+1)(n+2)$, ne sont pas des carrés (pour le second, $n+1$ et $n(n+2)$ le seraient).

Exercice 22 Triplets pythagoriciens ★★★

corrigé p. 49

On cherche les triplets $(x, y, z) \in \mathbb{N}^{*3}$ tels que $x^2 + y^2 = z^2$ et $x \wedge y = 1$ (triplets primitifs).

1. Montrer que x et y sont de parités différentes (modulo 4) ; on suppose désormais y pair.
2. Montrer que $x \wedge z = 1$, que $z \pm x$ sont pairs et que $\frac{z+x}{2} \wedge \frac{z-x}{2} = 1$. Avec l'exercice 21, en déduire qu'il existe $m > n \geq 1$ premiers entre eux, de parités différentes, tels que $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$.
3. Réciproquement, montrer que ces formules donnent toujours un triplet primitif.
4. Déterminer tous les couples $(x, y) \in \mathbb{N}^{*2}$ (primitifs ou non) tels que $x^2 + y^2 = 65^2$.

Exercice 23 Trois équations diophantiennes ★★★

corrigé p. 49

1. Montrer que $x^2 - y^2 = 2026$ n'a pas de solution dans $\mathbb{Z}^2$; résoudre dans $\mathbb{N}^2$: $x^2 - y^2 = 2027$ (premier).
2. Résoudre dans $\mathbb{N}^{*2}$ l'équation $1! + 2! + \dots + n! = m^2$.
3. Résoudre dans $\mathbb{N} \times \mathbb{Z}$ l'équation $2^x + 7 = y^2$.

18

Niveau 4 · Concours**Exercice 24** Autour de $2^n - 1$ et de $n \cdot 2^n + 1$ ★★★★★

corrigé p. 50

1. Soit $n \geq 2$ tel que $n \mid 2^n - 1$, et p son plus petit diviseur premier. a) Justifier que p est impair, et que l'ordre k de 2 modulo p (plus petit $k \geq 1$ tel que $2^k \equiv 1 [p]$) divise n et $p - 1$. b) En déduire que $k = 1$ et conclure : seul $n = 1$ vérifie $n \mid 2^n - 1$.
2. Déterminer les entiers naturels n tels que 3 divise $n \cdot 2^n + 1$.
3. Soit p un nombre premier impair. Montrer que, pour tout $m \in \mathbb{N}$, l'entier $n = (p - 1)(mp + 1)$ vérifie $p \mid n \cdot 2^n + 1$. Conclure.

Exercice 25 L'équation $y^2 = x^3 + 7$ ★★★★★

corrigé p. 50

On suppose par l'absurde qu'il existe $(x, y) \in \mathbb{Z}^2$ tel que $y^2 = x^3 + 7$.

1. Montrer que x est impair (raisonner modulo 8).
2. Vérifier que $y^2 + 1 = (x + 2)(x^2 - 2x + 4)$ et que $x^2 - 2x + 4 \equiv 3 [4]$.
3. En déduire que $y^2 + 1$ admet un diviseur premier $q \equiv 3 [4]$, et conclure à l'aide de l'exercice 20.

Exercice 26 L'identité de Sophie Germain ★★★★★

corrigé p. 50

1. Montrer que, pour tous entiers a et b : $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.
2. Montrer que, pour $n \in \mathbb{N}^*$, $n^4 + 4$ est premier si et seulement si $n = 1$, et que $n^4 + 64$ n'est jamais premier.
3. Montrer que $n^4 + 4^n$ ($n \in \mathbb{N}^*$) n'est premier que pour $n = 1$; ainsi $2027^4 + 4^{2027}$ est composé.

Exercice 27 Le principe du chiffrement RSA ★★★★★

corrigé p. 50

Soient p et q deux nombres premiers distincts, $N = pq$, $M = (p-1)(q-1)$ et $e \in \mathbb{N}^*$ premier avec M .

1. Justifier l'existence d'un entier $d \in \mathbb{N}^*$ tel que $ed \equiv 1 [M]$.
2. Soit $x \in \mathbb{Z}$. Montrer que $x^{ed} \equiv x [p]$ (distinguer les cas $p \mid x$ et $p \nmid x$). En déduire que $x^{ed} \equiv x [N]$.
3. Application : $p = 5$, $q = 11$, $e = 7$. a) Calculer N , M et le plus petit $d \in \mathbb{N}^*$ tel que $7d \equiv 1 [M]$. b) Le message $x = 13$ est codé par le reste y de x^7 modulo N . Calculer y , puis vérifier directement que $y^d \equiv 13 [N]$.

Exercice 28 Relèvement des exposants ★★★★★

corrigé p. 51

On reprend les valuations v_p de l'exercice 21.

1. Soient p premier impair et $a \in \mathbb{Z}$, $a \neq 1$, $a \equiv 1 [p]$. a) Montrer que $a^j \equiv 1 + j(a-1) [p^2]$ pour tout $j \in \mathbb{N}$. b) En déduire que $1 + a + \dots + a^{p-1} \equiv p [p^2]$, puis que $v_p(a^p - 1) = v_p(a - 1) + 1$. c) Montrer que $v_p(a^{p^j} - 1) = v_p(a - 1) + j$ pour tout $j \in \mathbb{N}$.
2. En déduire que, pour tout $j \in \mathbb{N}$: $v_5(2^{4 \cdot 5^j} - 1) = j + 1$ (prendre $a = 16$).
3. Soit $k \geq 1$. a) Montrer que $2^{4 \cdot 5^{k-1}} \equiv 1 [5^k]$ et $2^{2 \cdot 5^{k-1}} \equiv -1 [5]$. b) Montrer que le plus petit $\omega \geq 1$ tel que $2^\omega \equiv 1 [5^k]$ est $4 \cdot 5^{k-1}$. c) En déduire que tout entier non divisible par 5 est congru modulo 5^k à une puissance de 2.

Exercice 29 Le produit des nombres premiers ★★★★★

corrigé p. 51

Pour $n \geq 2$, $P(n)$ est le produit des premiers $p \leq n$ ($P(10) = 210$). On veut montrer que $P(n) < 4^n$.

1. Soit $m \in \mathbb{N}^*$. Montrer que $C_{2m+1}^m \leq 4^m$ (remarquer que $C_{2m+1}^m = C_{2m+1}^{m+1}$ et développer $(1+1)^{2m+1}$).
2. Montrer que tout nombre premier p tel que $m+2 \leq p \leq 2m+1$ divise C_{2m+1}^m . En déduire que $P(2m+1) \leq 4^m P(m+1)$.
3. Montrer par récurrence forte que $P(n) < 4^n$ pour tout $n \geq 2$.

Exercice 30 Les entiers n tels que n^2 divise $2^n + 1$ ★★★★★

corrigé p. 52

On cherche les $n \in \mathbb{N}^*$ tels que $n^2 \mid 2^n + 1$ (1 et 3 conviennent). Soit $n \geq 2$ une solution.

1. Soit p le plus petit diviseur premier de n . Montrer que p est impair, que $2^{2n} \equiv 1 [p]$, que l'ordre k de 2 modulo p divise 2, et que $p = 3$.
2. On écrit $n = 3^j m$, avec $j \geq 1$ et $3 \nmid m$. a) Montrer que m est impair et que $v_3(2^m + 1) = 1$ (utiliser $2^6 \equiv 1 [9]$). b) Avec l'exercice 28 (1.c, $a = (-2)^m$), montrer que $v_3(2^n + 1) = j + 1$; en déduire $j = 1$.
3. On suppose $m \geq 2$; soit q le plus petit diviseur premier de m . Montrer que $q \mid 2^6 - 1$, puis aboutir à une contradiction. Conclure.

Partie C • La banque

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

19 Division euclidienne

Pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple (q, r) tel que $a = bq + r$ et $0 \leq r < b$, et $q = E\left(\frac{a}{b}\right)$. On vérifie **toujours** la condition $0 \leq r < b$; pour un entier variable n , on raisonne par disjonction de cas selon son reste dans une division bien choisie.

Exercice 31 Quotient et reste : signes et cascades ★

corrigé p. 52

- On donne $2026 = 37 \times 54 + 28$. a) Justifier que cette égalité traduit la division euclidienne de 2026 par 37. b) Sans poser de nouvelle division, en déduire la division euclidienne de -2026 par 37, puis celles de 2026 et de -2026 par -37 (pour $b \in \mathbb{Z}^*$, on écrit $a = bq + r$ avec $0 \leq r < |b|$).
- Déterminer les entiers naturels b tels que le reste de la division euclidienne de 2026 par b soit égal à 26.
- Montrer que, si deux entiers ont le même reste dans la division euclidienne par $n \in \mathbb{N}^*$, alors n divise leur différence. Déterminer les entiers $n \geq 2$ tels que 2026, 1500 et 1237 aient le même reste dans la division euclidienne par n , et préciser ce reste.

Exercice 32 Changer de base ★

corrigé p. 53

On note $\overline{x_k \dots x_1 x_0}^{(b)} = x_k b^k + \dots + x_1 b + x_0$ ($0 \leq x_i \leq b - 1$, $x_k \neq 0$) ; en base 16, les chiffres 10, ..., 15 sont notés A, ..., F.

- Écrire en base dix les entiers $\overline{2026}^{(7)}$ et $\overline{101101}^{(2)}$.
- a) Soit $N = \overline{x_{3m+2} \dots x_1 x_0}^{(2)}$ (on complète au besoin par des zéros à gauche). Montrer que $N = \sum_{j=0}^m y_j 8^j$, où $y_j = \overline{x_{3j+2} x_{3j+1} x_{3j}}^{(2)}$, et en déduire une règle pour passer de la base 2 à la base 8. Énoncer la règle analogue pour la base 16. b) Écrire $N = \overline{101101110101}^{(2)}$ en base 8, en base 16, puis en base dix.
- Soit $b \geq 4$. Montrer que $\overline{121}^{(b)}$ est un carré et que $\overline{1331}^{(b)}$ est un cube. En déduire, sans division, l'écriture de 1000 en base 9 et celle de 343 en base 6.
- Écrire 2^{2026} en base 2, en base 8 et en base 16 (on pourra utiliser $2026 = 3 \times 675 + 1 = 4 \times 506 + 2$). Combien de chiffres a-t-il dans chacune de ces bases ?

Exercice 33 Quotients, restes et disjonction de cas ★★

corrigé p. 53

- Déterminer les entiers $n \in \mathbb{N}^*$ tels que, dans la division euclidienne de 2026 par n , le quotient soit égal au reste. (On vérifiera que 1013 est premier.)
- Déterminer, selon les valeurs de $n \in \mathbb{N}$, le quotient et le reste de la division euclidienne de $2^{n+3} + 5$ par $2^n + 1$.
- a) Montrer qu'un nombre premier $p \geq 5$ a pour reste 1 ou 5 dans la division euclidienne par 6.
b) En déduire que 24 divise $p^2 - 1$, puis que 24 divise $p^2 - q^2$ pour tous nombres premiers $p, q \geq 5$.

Exercice 34 Quotient et partie entière ★★

corrigé p. 54

On rappelle que le quotient de la division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{N}^*$ est $E\left(\frac{a}{b}\right)$.

- a) Soit $N, d \in \mathbb{N}^*$. Montrer que l'ensemble $\{1, 2, \dots, N\}$ contient exactement $E\left(\frac{N}{d}\right)$ multiples de d .
b) Justifier que $(6 \mid n \text{ et } 10 \mid n) \iff 30 \mid n$. Combien d'entiers de $\{1, \dots, 2026\}$ sont divisibles par 6 ou par 10 ?
- Soit $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$. En effectuant la division euclidienne de $E(x)$ par n , montrer que $E\left(\frac{E(x)}{n}\right) = E\left(\frac{x}{n}\right)$. En déduire $E\left(\frac{2026}{35}\right)$ à l'aide de deux divisions par des entiers à un chiffre.
- Soit $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Montrer que $\sum_{k=0}^{m-1} E\left(\frac{n+k}{m}\right) = n$ (on écrira $n = mq + r$). Vérifier pour $n = 2026$ et $m = 3$.
- Soit $a, b \in \mathbb{N}^*$ et $a = bq + r$ la division euclidienne de a par b . Montrer que, si $r < q$, alors la division euclidienne de a par q a pour quotient b et pour reste r . Application : diviser 2026 par 54 sans poser la division (utiliser l'exercice 31).

Exercice 35 Division centrée et pesées ★★★

corrigé p. 54

- Soit $m \in \mathbb{N}^*$ et $b = 2m + 1$. Montrer que, pour tout $a \in \mathbb{Z}$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $-m \leq r \leq m$ (division « centrée » de a par b). Effectuer la division centrée de 2026 par 29, sachant que $2026 = 29 \times 69 + 25$.
- Dans la suite, $b = 3$. Pour $k \in \mathbb{N}^*$, on pose $M_k = \frac{3^k - 1}{2}$. Montrer par récurrence sur k que tout entier n tel que $|n| \leq M_k$ s'écrit de façon unique $n = \sum_{i=0}^{k-1} \varepsilon_i 3^i$ avec $\varepsilon_i \in \{-1, 0, 1\}$ (écriture « ternaire équilibrée »).
- Donner l'écriture ternaire équilibrée de 2026 (on pourra partir de $3^7 = 2187$).
- On dispose d'une balance à deux plateaux et de cinq masses marquées de 1, 3, 9, 27 et 81 grammes, que l'on peut poser sur l'un ou l'autre plateau.
 - Montrer que l'on peut peser tout objet dont la masse est un nombre entier de grammes compris entre 1 et 121. Comment peser un objet de 100 g ?
 - Montrer qu'avec cinq masses marquées quelconques, on ne peut pas peser plus de 121 masses entières différentes.

Exercice 36 Le développement décimal de a/b ★★★

corrigé p. 55

Soit $b \geq 2$ et $a \in \{1, \dots, b-1\}$. On pose $r_0 = a$ puis, pour tout $k \in \mathbb{N}$, on note c_{k+1} et r_{k+1} le quotient et le reste de la division euclidienne de $10 r_k$ par b : $10 r_k = b c_{k+1} + r_{k+1}$, $0 \leq r_{k+1} \leq b-1$.

1. Montrer que $c_k \in \{0, 1, \dots, 9\}$ pour tout $k \geq 1$.
2. Montrer par récurrence que, pour tout $n \in \mathbb{N}^*$, $10^n a = b N_n + r_n$, où $N_n = \overline{c_1 c_2 \dots c_n}^{(10)} = \sum_{k=1}^n c_k 10^{n-k}$. En déduire que $\frac{N_n}{10^n} \leq \frac{a}{b} < \frac{N_n + 1}{10^n}$: $c_1, \dots, c_n$ sont les n premières décimales de $\frac{a}{b}$.
3. Calculer $r_1, \dots, r_6$ et $c_1, \dots, c_6$ pour $\frac{a}{b} = \frac{1}{7}$. Quelle est la 2026^e décimale de $\frac{1}{7}$?
4. On suppose qu'aucun r_k n'est nul. Montrer qu'il existe $i < j \leq b-1$ tels que $r_i = r_j$, puis que, avec $T = j - i$, on a $r_{k+T} = r_k$ et $c_{k+1+T} = c_{k+1}$ pour tout $k \geq i$. Que peut-on dire du développement décimal de $\frac{a}{b}$?
5. On suppose de plus $b \wedge 10 = 1$. a) Montrer qu'aucun r_n n'est nul, et que $r_{k+1} = r_{l+1}$ entraîne $r_k = r_l$. b) En déduire que $r_T = r_0$: le développement est périodique dès la première décimale. c) Calculer le développement de $\frac{1}{13}$. Celui de $\frac{1}{12}$ est-il périodique dès la première décimale ?

20

Congruences et restes

Calculer modulo n , c'est remplacer chaque nombre par un nombre plus simple qui lui est congru (compatibilité avec $+$, $\times$ et les puissances). Pour une grande puissance, on cherche une petite puissance congrue à 1 (ou à -1), puis on divise l'exposant ; pour une équation, on dresse un tableau de restes.

Exercice 37 Restes de grandes puissances ★

corrigé p. 56

1. Déterminer le reste de la division euclidienne : a) de 2^{2026} par 9 ; b) de $3^{100} + 4^{100}$ par 7 ; c) de 2026^{2027} par 17 (on calculera 3^4 et 3^8 modulo 17).
2. a) Vérifier que $13^4 \equiv 61 [100]$, puis que $13^{20} \equiv 1 [100]$. b) En déduire les deux derniers chiffres de 13^{2026} .
3. Montrer que, pour tout $n \in \mathbb{N}$, l'entier $6^{2n} + 3^{n+2} + 3^n$ est divisible par 11.

Exercice 38 Tableaux de restes et équations ★

corrigé p. 56

1. Dresser le tableau des restes de x^2 modulo 13 pour $x \in \{0, 1, \dots, 12\}$. Quels sont les restes possibles d'un carré dans la division par 13 ?
2. Résoudre dans $\mathbb{Z}$: a) $5x \equiv 7 [13]$; b) $x^2 + 4x \equiv 6 [13]$ (écrire $x^2 + 4x = (x+2)^2 - 4$) ; c) $2x^2 + 3x + 4 \equiv 0 [13]$ (multiplier par 8 pour faire apparaître $(4x+3)^2$).
3. a) Montrer que l'équation $x^2 - 13y = 2$ n'a pas de solution dans $\mathbb{Z}^2$. b) Résoudre dans $\mathbb{Z}^2$ l'équation $x^2 - 13y = 3$.

Exercice 39 Critères de divisibilité ★★

corrigé p. 57

1. a) Vérifier que $999 = 27 \times 37$. Un entier naturel N est découpé, à partir de la droite, en tranches de trois chiffres : $N = t_0 + 1000 t_1 + 1000^2 t_2 + \dots$ avec $0 \leq t_i \leq 999$. Montrer que $N \equiv t_0 + t_1 + t_2 + \dots \pmod{999}$, et en déduire un critère de divisibilité par 37 et un critère de divisibilité par 27.
b) Déterminer les restes de 123 456 789 dans la division par 37 et dans la division par 27.
2. Tout entier $N \geq 10$ s'écrit $N = 10a + u$, où u est son chiffre des unités. a) Montrer que $2N \equiv a + 2u \pmod{19}$, puis que $19 \mid N \iff 19 \mid a + 2u$. b) En itérant ce critère, montrer que 87 723 est divisible par 19, mais que 2026 ne l'est pas.
3. On note $S(N)$ la somme des chiffres (en base dix) de l'entier naturel N . a) Rappeler pourquoi $N \equiv S(N) \pmod{9}$. b) Déterminer tous les entiers naturels N tels que $N + S(N) = 2026$.

Exercice 40 Puissances de 2 modulo 31 ★★

corrigé p. 57

1. Vérifier que $2^5 \equiv 1 \pmod{31}$, puis déterminer, suivant les valeurs de l'entier naturel n , le reste de 2^n dans la division par 31.
2. Déterminer le reste de $2^{2026} + 33^{2027}$ dans la division par 31.
3. Pour $n \in \mathbb{N}$, on pose $A_n = 1 + 2^n + 4^n + 8^n + 16^n$. a) Montrer que $31 \mid A_n$ si et seulement si $n \neq 0 \pmod{5}$.
b) Retrouver le sens « $\Leftarrow$ » en calculant $(2^n - 1)A_n$ (on rappelle que 31 est premier).
4. Déterminer les entiers naturels n tels que $2^n \equiv n \pmod{31}$ (on écrira $n = 5k + r$ et l'on remarquera que $31 \equiv 1 \pmod{5}$).

Exercice 41 Calendrier et congruences ★★

corrigé p. 58

Dans le calendrier grégorien, une année compte 365 jours, sauf les années bissextiles (366 jours, avec un 29 février) : celles dont le millésime est divisible par 4, à l'exception de celles qui sont divisibles par 100 sans l'être par 400. Les jours de la semaine sont repérés modulo 7.

1. Justifier que, d'une date à la même date de l'année suivante, le jour de la semaine avance d'un rang, ou de deux rangs si un 29 février a été franchi.
2. Le 14 octobre 2026 est un mercredi. Quel jour de la semaine sera le 14 octobre 2126 ?
3. Montrer que 400 années consécutives comptent exactement 146 097 jours, et en déduire que le calendrier grégorien se répète, jours de la semaine compris, tous les 400 ans.
4. Pour $1 \leq m \leq 12$, on note d_m le nombre de jours qui séparent le 13 janvier du 13 du m -ième mois de la même année ($d_1 = 0$). a) Déterminer les restes de $d_1, \dots, d_{12}$ modulo 7, pour une année non bissextile puis pour une année bissextile. b) En déduire que toute année compte au moins un vendredi 13, et au plus trois. Sachant que le 13 février 2026 est un vendredi, quels sont les vendredis 13 de l'année 2026 ?

Exercice 42 Le chiffre des unités de n^n ★★★

corrigé p. 58

Pour $n \in \mathbb{N}^*$, on note u_n le chiffre des unités de n^n .

1. Justifier, à l'aide d'un résultat du cours, que $n^5 \equiv n \pmod{10}$ pour tout $n \in \mathbb{Z}$. En déduire que $n^{k+4} \equiv n^k \pmod{10}$ pour tous $n \in \mathbb{Z}$ et $k \in \mathbb{N}^*$, puis que $n^{k+4j} \equiv n^k \pmod{10}$ pour tout $j \in \mathbb{N}$.
2. Montrer que $u_{n+20} = u_n$ pour tout $n \in \mathbb{N}^*$.
3. Calculer $u_1, u_2, \dots, u_{20}$ et leur somme. La suite (u_n) admet-elle 10 pour période ?

4. Déterminer le chiffre des unités de $S = 1^1 + 2^2 + 3^3 + \dots + 2026^{2026}$.

21 PGCD et théorème de Bézout

Le lemme $a \wedge b = (a - kb) \wedge b$ justifie l'algorithme d'Euclide et donne le PGCD d'expressions en n . Le théorème de Bézout ($a \wedge b = 1 \iff au + bv = 1$ pour certains $u, v \in \mathbb{Z}$) fournit les inverses modulo n ; on le combine avec le théorème de Gauss.

Exercice 43 Euclide et carrelage ★

corrigé p. 59

1. a) À l'aide de l'algorithme d'Euclide, calculer $1512 \wedge 1092$. b) En déduire les diviseurs communs positifs de 1512 et 1092, ainsi que la forme irréductible de $\frac{1092}{1512}$. c) Retrouver ce PGCD à l'aide des décompositions en facteurs premiers.
2. Une salle rectangulaire de 15,12 m sur 10,92 m doit être recouverte, sans découpe, de carreaux carrés identiques dont le côté est un nombre entier de centimètres. Quel est le plus grand côté possible ? Combien faut-il alors de carreaux ?
3. *Euclide par soustractions.* Montrer que, pour $a > b \geq 1$, $a \wedge b = (a - b) \wedge b$. On remplace à chaque étape le plus grand des deux nombres par leur différence, jusqu'à obtenir deux nombres égaux. Combien de soustractions faut-il en partant de (1512, 1092) ? Exprimer ce nombre à l'aide des quotients obtenus en 1.a).

Exercice 44 PGCD d'expressions en n ★

corrigé p. 59

1. Montrer que, pour tout $n \in \mathbb{N}^*$, la fraction $\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$ est irréductible.
2. Montrer que $(n + 1) \wedge (n^2 + 1) \in \{1, 2\}$ ($n \in \mathbb{N}^*$), et préciser sa valeur selon n .
3. Montrer que $(n! + 1) \wedge ((n + 1)! + 1) = 1$ pour tout $n \in \mathbb{N}^*$. Le résultat reste-t-il vrai pour $n = 0$?

Exercice 45 Les deux récipients ★★

corrigé p. 60

On dispose d'une fontaine et de deux récipients non gradués de a et b litres ($a, b \in \mathbb{N}^*$). Les seules opérations permises sont : remplir un récipient à la fontaine, vider un récipient, transvaser l'un dans l'autre jusqu'à ce que le premier soit vide ou le second plein.

1. Montrer, par récurrence sur le nombre d'opérations, que la quantité d'eau contenue dans chaque récipient est toujours un multiple de $a \wedge b$. Peut-on obtenir exactement 1 litre avec des récipients de 9 et 6 litres ?
2. Dans la suite, A contient 9 litres et B en contient 7. À l'aide de l'algorithme d'Euclide, trouver $(u, v) \in \mathbb{N}^2$ tel que $7u - 9v = 1$. Interpréter à l'aide des récipients.
3. On applique le procédé : « remplir B et le transvaser dans A ; chaque fois que A est plein, le vider puis poursuivre le transvasement ». On note r_k la quantité contenue dans A juste après le k -ième vidage complet de B ($r_0 = 0$).
 - a) Montrer que r_k est le reste de la division euclidienne de $7k$ par 9.
 - b) Montrer que $r_1, \dots, r_8$ sont les entiers $1, \dots, 8$ dans un certain ordre. Que peut-on en conclure ?
 - c) Combien de remplissages de B faut-il pour obtenir 4 litres dans A ? Et combien de remplissages de A pour obtenir 4 litres dans B si l'on échange les rôles de A et B ?

Exercice 46 Premiers entre eux ★★

corrigé p. 60

1. Soit $a, b \in \mathbb{Z}$ non tous deux nuls et $d = a \wedge b$. Montrer que $a^2 \wedge b^2 = d^2$.
2. Soit $a, b \in \mathbb{Z}$ premiers entre eux, avec $a + b \neq 0$, et $\delta = (a + b) \wedge (a^2 - ab + b^2)$. a) Montrer que $\delta \wedge a = \delta \wedge b = 1$, puis que $\delta \wedge ab = 1$. b) En écrivant $a^2 - ab + b^2 = (a + b)^2 - 3ab$, montrer que $\delta \mid 3$. Conclure : $\delta = 3$ si $3 \mid a + b$, et $\delta = 1$ sinon. c) Application : calculer δ pour $(a, b) = (2026, 1)$ et pour $(a, b) = (5, 4)$, sachant que $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$.
3. Montrer que, pour tout $n \in \mathbb{N}$, $(n^2 + 2) \wedge ((n + 1)^2 + 2) \in \{1, 3, 9\}$, et préciser pour quels n il vaut 3, puis 9.
4. Montrer que, pour tout $n \in \mathbb{N}$, $(2^n + 3^n) \wedge (2^{n+1} + 3^{n+1}) = 1$.

Exercice 47 Fractions voisines ★★★

corrigé p. 61

Deux fractions $\frac{a}{b} < \frac{c}{d}$ ($a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}^*$) sont dites *voisines* si $bc - ad = 1$.

1. Montrer que deux fractions voisines sont irréductibles, et que leur *médiane* $\frac{a+c}{b+d}$ est irréductible, strictement comprise entre $\frac{a}{b}$ et $\frac{c}{d}$, et voisine de chacune d'elles.
2. Soit $\frac{p}{q}$ ($q \in \mathbb{N}^*$) telle que $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$. a) Montrer que $pb - aq \geq 1$ et $cq - pd \geq 1$, puis établir l'identité $d(pb - aq) + b(cq - pd) = q$. b) En déduire que $q \geq b + d$, avec égalité si et seulement si $\frac{p}{q} = \frac{a+c}{b+d}$.
3. a) Vérifier que $\frac{13}{18}$ et $\frac{8}{11}$ sont voisines. Quelle est la fraction de plus petit dénominateur strictement comprise entre elles ? b) À l'aide du théorème de Bézout, montrer que toute fraction irréductible $\frac{a}{b}$ avec $b \geq 2$ admet une voisine $\frac{c}{d} > \frac{a}{b}$ telle que $1 \leq d \leq b - 1$. Retrouver $\frac{8}{11}$ à partir de $\frac{13}{18}$.
4. Le taux de réussite aux tirs d'un basketballer est strictement compris entre 72 % et 73 %. Vérifier que $\frac{5}{7} < \frac{72}{100} < \frac{8}{11} < \frac{73}{100} < \frac{3}{4}$ et que $\frac{8}{11}$ est voisine de $\frac{5}{7}$ et de $\frac{3}{4}$. En déduire le nombre minimal de tirs qu'il a tentés.

Exercice 48 Une somme de parties entières ★★★

corrigé p. 62

Soit $a \in \mathbb{N}^*$, $b \geq 2$ et $S(a, b) = \sum_{k=1}^{b-1} E\left(\frac{ka}{b}\right)$.

1. On suppose $a \wedge b = 1$ et l'on note r_k le reste de la division de ka par b ($1 \leq k \leq b - 1$). a) Montrer que les r_k sont non nuls et deux à deux distincts ; en déduire que $\{r_1, \dots, r_{b-1}\} = \{1, \dots, b - 1\}$. b) En sommant les égalités $ka = bE\left(\frac{ka}{b}\right) + r_k$, montrer que $S(a, b) = \frac{(a-1)(b-1)}{2}$.
2. Dans un repère, on considère le rectangle $[0, b] \times [0, a]$ et sa diagonale D d'extrémités O et $B(b, a)$. Un point est *entier* si ses coordonnées sont entières. a) Montrer que $S(a, b)$ est le nombre de points entiers intérieurs au rectangle et situés sous D ou sur D . b) On suppose $a \wedge b = 1$. Montrer qu'aucun point entier intérieur au rectangle n'est sur D , puis retrouver $S(a, b)$ par une symétrie. Illustrer avec $a = 5$, $b = 8$.
3. Cas général : soit $d = a \wedge b$. Montrer que D contient exactement $d - 1$ points entiers intérieurs au rectangle, puis que $S(a, b) = \frac{(a-1)(b-1) + d - 1}{2}$.

4. Calculer $\sum_{k=1}^{11} E\left(\frac{8k}{12}\right)$ et $\sum_{k=1}^{2025} E\left(\frac{1155k}{2026}\right)$.

22 Gauss et nombres premiers

Théorème de Gauss, lemme d'Euclide et décomposition en facteurs premiers : trois outils pour résoudre des équations produits, compter des diviseurs et raisonner sur les nombres premiers.

Exercice 49 Premiers ou pas ? ★

corrigé p. 63

- Montrer que 643 est un nombre premier.
 - L'entier 667 est-il premier ?
- Soit p premier tel que $p + 10$ et $p + 14$ soient premiers. Montrer (modulo 3) que $p = 3$, et vérifier que $p = 3$ convient.
- Pour $n \in \mathbb{N}$, on pose $f(n) = n^2 + n + 41$.
 - Vérifier que $f(0), f(1), \dots, f(5)$ sont premiers.
 - Montrer, à l'aide de tableaux de restes, que $f(n)$ n'est divisible ni par 2, ni par 3, ni par 5, ni par 7.
 - Montrer que $f(n) \equiv n(n+1) \pmod{41}$, puis (lemme d'Euclide) que $41 \mid f(n) \iff n \equiv 0 \text{ ou } 40 \pmod{41}$.
 - Calculer $f(40)$ et $f(41)$. L'entier $f(n)$ est-il premier pour tout n ?

Exercice 50 Les engrenages ★

corrigé p. 63

Deux roues dentées A (72 dents) et B (54 dents) sont engrenées ; une dent de A et une dent de B, marquées d'un repère, sont en contact à l'instant initial. Les dents de B sont numérotées de 0 à 53 dans leur ordre de passage au point de contact, la dent marquée portant le numéro 0.

- Décomposer 72 et 54 en facteurs premiers ; en déduire $72 \wedge 54$ et le PPCM de 72 et 54.
- Lorsque A a fait x tours et B en a fait y ($x, y \in \mathbb{N}$), le même nombre de dents est passé au point de contact. Résoudre dans $\mathbb{N}^2$ l'équation $72x = 54y$ (théorème de Gauss).
- Au bout de combien de tours de chaque roue les deux repères se retrouvent-ils pour la première fois en contact ? Combien de dents sont alors passées ?
- Chaque fois que la dent marquée de A revient au point de contact, elle rencontre une dent de B. Montrer qu'elle ne rencontre que trois dents de B et donner leurs numéros.
- Une troisième roue C de 90 dents engrène avec B. Au bout de combien de tours de chaque roue les trois roues retrouvent-elles simultanément, pour la première fois, leur position initiale ?

Exercice 51 Racines rationnelles d'un polynôme ★★

corrigé p. 64

Soit $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ un polynôme à coefficients entiers, avec $n \geq 1$, $a_n \neq 0$ et $a_0 \neq 0$. On suppose que le rationnel $r = \frac{p}{q}$, avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$, est une racine de P .

- Montrer que $p \mid a_0 q^n$ et $q \mid a_n p^n$. En déduire (Gauss) que $p \mid a_0$ et $q \mid a_n$.
- Application. On pose $P(x) = 6x^3 - 11x^2 - 3x + 2$.
 - Dresser la liste des rationnels susceptibles d'être racines de P .
 - Déterminer les racines rationnelles de P , puis factoriser $P(x)$.
- On pose $\alpha = \sqrt{3} + \sqrt{5}$. Montrer que $\alpha^4 - 16\alpha^2 + 4 = 0$, puis que α est irrationnel.

4. Soit $m \in \mathbb{N}$ tel que $\sqrt[3]{m}$ soit rationnel. Montrer que m est le cube d'un entier. Et $\sqrt[3]{12}$?

Exercice 52 Diviseurs : compter et multiplier ★★

corrigé p. 64

Pour $n \in \mathbb{N}^*$, on note $d(n)$ le nombre de diviseurs positifs de n et $\Pi(n)$ leur produit.

- On pose $N = 5292$.
 - Décomposer N en facteurs premiers et calculer $d(N)$.
 - Combien N a-t-il de diviseurs pairs ? de diviseurs qui sont des carrés parfaits ?
 - Déterminer le plus petit entier $k \geq 1$ tel que kN soit un carré parfait, puis le plus petit entier $k \geq 1$ tel que kN soit un cube parfait.
- Montrer que $\delta \mapsto \frac{n}{\delta}$ est une bijection de l'ensemble des diviseurs positifs de n sur lui-même. En déduire que $\Pi(n)^2 = n^{d(n)}$.
 - Écrire $\Pi(N)$ comme une puissance de N , puis donner sa décomposition en facteurs premiers.
- Soit $n \geq 2$. Montrer que $\Pi(n) = n^3 \iff d(n) = 6 \iff n = p^5$ ou $n = p^2q$ (p, q premiers distincts).
 - Déterminer les entiers n tels que $2 \leq n \leq 50$ et $\Pi(n) = n^3$.
- Montrer que $d(n) < 2\sqrt{n}$ pour tout $n \in \mathbb{N}^*$ (associer à chaque diviseur $\delta < \sqrt{n}$ le diviseur $\frac{n}{\delta}$).

Exercice 53 Une infinité de premiers de la forme $4k + 3$ ★★★

corrigé p. 65

- Montrer qu'un produit d'entiers tous congrus à 1 modulo 4 est congru à 1 modulo 4.
- Soit $n \in \mathbb{N}$ tel que $n \equiv 3 \pmod{4}$. Montrer que n a un diviseur premier $p \equiv 3 \pmod{4}$.
- On suppose qu'il n'y a qu'un nombre fini de premiers congrus à 3 modulo 4, notés $p_1, \dots, p_k$, et on pose $N = 4p_1 \cdots p_k - 1$. Aboutir à une contradiction.
- Montrer que tout nombre premier $p \geq 5$ vérifie $p \equiv 1 \pmod{6}$ ou $p \equiv 5 \pmod{6}$.
 - En adaptant la méthode, montrer qu'il existe une infinité de premiers congrus à 5 modulo 6.
- Pourquoi la méthode ne s'adapte-t-elle pas aux premiers congrus à 1 modulo 4 ? (Penser à 21.)

Exercice 54 Les nombres parfaits pairs ★★★

corrigé p. 65

Pour $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs positifs de n . On dit que n est *parfait* si $\sigma(n) = 2n$.

- Vérifier que 6 et 28 sont parfaits. Montrer que, si p est premier et $a \in \mathbb{N}$, alors $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$.
- Soit $a, b \in \mathbb{N}^*$ tels que $a \wedge b = 1$.
 - Soit d un diviseur positif de ab , $d_1 = d \wedge a$ et $d_2 = \frac{d}{d_1}$. Montrer que $d_2 \mid b$ (Gauss).
 - Montrer que, si $d_1 d_2 = d'_1 d'_2$ avec d_1, d'_1 diviseurs positifs de a et d_2, d'_2 de b , alors $d_1 = d'_1$ et $d_2 = d'_2$. En déduire $\sigma(ab) = \sigma(a)\sigma(b)$.
- Théorème d'Euclide.** Soit $k \geq 2$ tel que $M = 2^k - 1$ soit premier, et $n = 2^{k-1}M$. Montrer que n est parfait. Donner les quatre plus petits nombres parfaits ainsi obtenus.
- On garde les notations de la question 3.

- Montrer que $n = 1 + 2 + 3 + \dots + M$.
- On suppose k impair et $k \geq 3$. Montrer que $n \equiv 1 [9]$ (on pourra utiliser $2^6 \equiv 1 [9]$).
- Sachant (cours) que k est premier, montrer que le chiffre des unités de n est 6 ou 8.

23

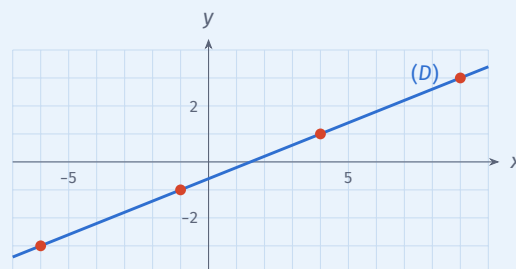
Équations diophantiennes

Résoudre en nombres entiers, c'est chercher des points à coordonnées entières : Bézout donne l'existence, Gauss toutes les solutions, et la factorisation règle bien des équations non linéaires.

Exercice 55 Lire puis prouver ★

corrigé p. 66

La figure ci-contre représente, dans un repère orthonormé, la droite (D) d'équation $2x - 5y = 3$.



- Lire sur la figure les points de (D) à coordonnées entières. Par quel vecteur passe-t-on de l'un au suivant ? Quelle est leur distance ?
- Démontrer que les solutions dans $\mathbb{Z}^2$ de l'équation $2x - 5y = 3$ sont les couples $(4 + 5k, 1 + 2k)$, $k \in \mathbb{Z}$.
- Combien la droite (D) possède-t-elle de points à coordonnées entières dans le carré $[-50, 50]^2$?
- Déterminer le point de (D) à coordonnées entières le plus proche de l'origine O .

Exercice 56 Au club de sport ★

corrigé p. 67

Un club achète des ballons à 120 dirhams l'unité et des maillots à 75 dirhams l'unité ; il dépense exactement 1995 dirhams. On note x le nombre de ballons et y le nombre de maillots achetés.

- Calculer $120 \wedge 75$ et montrer que $8x + 5y = 133$.
- Vérifier que $(1, 25)$ est une solution, puis résoudre dans $\mathbb{Z}^2$ l'équation $8x + 5y = 133$.
- Déterminer toutes les possibilités d'achat.
- Le club veut au moins autant de ballons que de maillots, et le plus d'articles possible. Que doit-il acheter ?
- Pour un autre achat de ce type, le vendeur annonce 1990 dirhams. Pourquoi est-ce forcément une erreur ?

Exercice 57 Type examen : quand le PGCD s'en mêle ★★

corrigé p. 67

On considère dans $\mathbb{Z}^2$ l'équation (E) : $77x - 105y = 28$.

- Calculer $77 \wedge 105$ et montrer que (E) équivaut à $11x - 15y = 4$.
 - Vérifier que $(14, 10)$ est une solution de (E) , puis résoudre (E) .
- Soit (x, y) une solution de (E) et $\delta = x \wedge y$.
 - Montrer que $\delta \in \{1, 2, 4\}$.
 - On écrit $x = 14 + 15k$ et $y = 10 + 11k$, $k \in \mathbb{Z}$. Déterminer δ suivant les valeurs de k .
- Résoudre dans $\mathbb{Z}$ l'équation $77x \equiv 28 [105]$.
- Déterminer les entiers n tels que $n \equiv 2 [11]$ et $n \equiv 6 [15]$.

b) Quel est le plus petit d'entre eux supérieur à 2026 ?

Exercice 58 Factoriser pour résoudre ★★

corrigé p. 67

- a) Vérifier que, pour tous réels x et y : $(2x + 5)(2y - 3) = 2(2xy - 3x + 5y) - 15$.

b) Résoudre dans $\mathbb{Z}^2$ l'équation $2xy - 3x + 5y = 22$.
- Factoriser $x^2 - xy - 2y^2$, puis résoudre dans $\mathbb{Z}^2$ l'équation $x^2 - xy - 2y^2 = 7$.
- On cherche les triangles rectangles à côtés entiers dont l'aire est égale au périmètre ; on note $a \leq b$ les côtés de l'angle droit et c l'hypoténuse.
 - Montrer que $c = \frac{ab}{2} - a - b$, puis, à l'aide du théorème de Pythagore, que $(a - 4)(b - 4) = 8$.
 - En déduire tous les triangles cherchés.

Exercice 59 Une équation à trois inconnues ★★★

corrigé p. 68

On considère l'équation (E) : $6x + 10y + 15z = 1$, d'inconnue $(x, y, z) \in \mathbb{Z}^3$.

- Calculer $6 \wedge 10$, $6 \wedge 15$, $10 \wedge 15$. Les équations $6x + 10y = 1$, $6x + 15z = 1$, $10y + 15z = 1$ ont-elles des solutions dans $\mathbb{Z}^2$? Vérifier que $(1, 1, -1)$ est solution de (E).
- a) Soit (x, y, z) une solution de (E). Montrer que z est impair, puis qu'en écrivant $z = 1 + 2t$ ($t \in \mathbb{Z}$), on a $3x + 5y = -7 - 15t$.

b) En déduire que les solutions de (E) sont les triplets $(-4 + 5s - 5t, 1 - 3s, 1 + 2t)$, $(s, t) \in \mathbb{Z}^2$.
- On dit qu'un entier naturel n est *représentable* s'il existe $(x, y, z) \in \mathbb{N}^3$ tel que $6x + 10y + 15z = n$.
 - Montrer que 29 n'est pas représentable.
 - Montrer que 30, 31, ..., 35 sont représentables, puis que tout entier $n \geq 30$ est représentable.

Exercice 60 Le problème des timbres ★★★

corrigé p. 68

Soit $a, b \geq 2$ deux entiers premiers entre eux. Avec des timbres de a et de b dirhams (en quantité illimitée), un montant $n \in \mathbb{N}$ est *affranchissable* s'il existe $(x, y) \in \mathbb{N}^2$ tel que $n = ax + by$. On pose $g = ab - a - b$.

- a) Montrer que tout entier n s'écrit de façon unique $n = ax + by$ avec $x \in \{0, 1, \dots, b-1\}$ et $y \in \mathbb{Z}$.

b) Montrer que $n \in \mathbb{N}$ est affranchissable si et seulement si, dans cette écriture, $y \geq 0$.
- Montrer que g n'est pas affranchissable, mais que tout entier $n > g$ l'est.
- a) Soit $n \in \{0, 1, \dots, g\}$. Montrer que n est affranchissable si et seulement si $g - n$ ne l'est pas.

b) En déduire qu'il y a exactement $\frac{(a-1)(b-1)}{2}$ montants non affranchissables.
- Application.* Avec des timbres de 5 et de 9 dirhams, quel est le plus grand montant non affranchissable ? Combien y a-t-il de montants non affranchissables ? Les énumérer.

24

Défis de concours

Six problèmes de concours et d'olympiades : chaque question prépare la suivante.

Exercice 61 Le théorème de Wilson ★★★★★

corrigé p. 69

Soit p un nombre premier.

- Montrer que, pour tout $a \in \{1, \dots, p-1\}$, il existe un unique $a' \in \{1, \dots, p-1\}$ tel que $aa' \equiv 1 [p]$.
 - Montrer que $a' = a$ si et seulement si $a = 1$ ou $a = p-1$.
- En déduire le *théorème de Wilson* : $(p-1)! \equiv -1 [p]$.
- Soit $n \geq 2$ non premier. Montrer que $(n-1)! \not\equiv -1 [n]$. Conclure : $n \geq 2$ est premier $\iff n \mid (n-1)! + 1$.
- Sachant que 101 est premier, déterminer le reste de $97!$ modulo 101.
- On suppose $p \equiv 1 [4]$ et on écrit $p = 4m + 1$.
 - Montrer que $(p-1)! \equiv ((2m)!)^2 [p]$ (associer j et $p-j$), puis que $((2m)!)^2 \equiv -1 [p]$.
 - Application. Déterminer les entiers $x \in \{0, \dots, 12\}$ tels que $x^2 \equiv -1 [13]$.

Exercice 62 Sommes de deux carrés ★★★★★

corrigé p. 70

On note S l'ensemble des entiers de la forme $a^2 + b^2$, avec $(a, b) \in \mathbb{Z}^2$.

- Vérifier que $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. En déduire que S est stable par produit et écrire $221 = 13 \times 17$ de deux façons comme somme de deux carrés.
- Soit p un nombre premier tel que $p \equiv 3 [4]$. On admet (exercice 20) que l'équation $x^2 \equiv -1 [p]$ n'a pas de solution.
 - Montrer que, si $p \mid a^2 + b^2$, alors $p \mid a$ et $p \mid b$.
 - En déduire que, si $n \in S$ et $n \neq 0$, l'exposant de p dans la décomposition de n est pair. L'entier $2001 = 3 \times 23 \times 29$ est-il dans S ?
- Lemme de Thue*. Soit $p \equiv 1 [4]$ premier, m tel que $m^2 \equiv -1 [p]$ (exercice 61), $q = E(\sqrt{p})$.
 - On considère les $(q+1)^2$ entiers $x - my$, avec $x, y \in \{0, 1, \dots, q\}$. Montrer que deux d'entre eux, associés à des couples distincts (x_1, y_1) et (x_2, y_2) , ont le même reste modulo p .
 - On pose $a = x_1 - x_2$, $b = y_1 - y_2$. Montrer que $a \equiv mb [p]$, $p \mid a^2 + b^2$, $0 < a^2 + b^2 < 2p$. Conclure.
- Application. Vérifier que $12^2 \equiv -1 [29]$ et écrire 29 comme somme de deux carrés par la méthode de 3. Écrire aussi 2029 (premier), puis 13×2029 (de deux façons), comme sommes de deux carrés.

Exercice 63 Indicatrice et théorème d'Euler ★★★★★

corrigé p. 70

Pour $n \geq 2$, on note $\varphi(n)$ le nombre d'entiers $k \in \{1, \dots, n\}$ tels que $k \wedge n = 1$.

- Calculer $\varphi(12)$ et $\varphi(p)$ pour p premier. Montrer que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ si p est premier et $\alpha \in \mathbb{N}^*$.
- Théorème d'Euler*. Soit $n \geq 2$, $N = \varphi(n)$, $r_1, \dots, r_N$ les éléments de $\{1, \dots, n\}$ premiers avec n , et a un entier tel que $a \wedge n = 1$. On note s_i le reste de ar_i modulo n .
 - Montrer que $s_i \wedge n = 1$ et que $s_i \neq s_j$ pour $i \neq j$.

- b) En déduire que $\{s_1, \dots, s_N\} = \{r_1, \dots, r_N\}$, puis que $a^{\varphi(n)} \equiv 1 [n]$. Cas n premier ?
3. a) Montrer que $\varphi(1000) = 400$ en comptant les entiers de $\{1, \dots, 1000\}$ divisibles par 2 ou par 5.
- b) Déterminer les trois derniers chiffres de 11^{2026} (on pourra développer $(10 + 1)^{26}$).
4. Calculer $\varphi(100)$ et $\varphi(40)$. En déduire le reste de 3^{2026} modulo 40, puis les deux derniers chiffres de 3^{2026} .

Exercice 64 Les nombres de Carmichael ★★★★★

corrigé p. 71

Un entier $n \geq 2$ non premier est un nombre de Carmichael si $a^n \equiv a [n]$ pour tout $a \in \mathbb{Z}$.

- Soit p premier et $n \geq 2$ tel que $(p-1) \mid (n-1)$. Montrer que $a^n \equiv a [p]$ pour tout $a \in \mathbb{Z}$.
- Critère de Korselt.* Soit $n = p_1 p_2 \cdots p_k$ ($k \geq 2$), produit de nombres premiers distincts tels que $(p_i - 1) \mid (n - 1)$ pour tout i . Montrer que n est un nombre de Carmichael.
- Montrer que 561, 1105 et 1729 sont des nombres de Carmichael.
- Soit n un nombre de Carmichael. Montrer que n est impair (prendre $a = n - 1$), puis que n n'est divisible par le carré d'aucun nombre premier (prendre $a = p$).
- Familles de Chernick.* Soit $k \in \mathbb{N}^*$ tel que $6k + 1$, $12k + 1$ et $18k + 1$ soient premiers. Montrer que $n = (6k + 1)(12k + 1)(18k + 1)$ est un nombre de Carmichael. Cas $k = 1$ et $k = 6$?

Exercice 65 Puissances de 2 et de 3 voisines ★★★★★

corrigé p. 72

- Résoudre dans $\mathbb{N}^2$ l'équation $2^a - 3^b = 1$ (pour $b \geq 1$, étudier 2^a modulo 3, puis factoriser).
- Résoudre dans $\mathbb{N}^2$ l'équation $3^b - 2^a = 1$ (pour $a \geq 2$, étudier 3^b modulo 4).
- Applications.* Déterminer les entiers naturels n tels que :
 - $1 + 2 + 2^2 + \cdots + 2^n$ soit une puissance de 3 ;
 - $1 + 3 + 3^2 + \cdots + 3^n$ soit une puissance de 2.
- Résoudre dans $\mathbb{N}^2$ l'équation $2^a - 3^b = 7$ (on pourra raisonner modulo 3 et modulo 8).

Exercice 66 Les restes chinois ★★★★★

corrigé p. 72

- Soit $k \geq 2$, $m_1, \dots, m_k \geq 2$ des entiers premiers entre eux deux à deux, $M = m_1 \cdots m_k$ et $r_1, \dots, r_k \in \mathbb{Z}$.
 - Montrer que $m_k \wedge (m_1 \cdots m_{k-1}) = 1$.
 - Montrer par récurrence sur k que les solutions du système $x \equiv r_i [m_i]$ ($1 \leq i \leq k$) forment exactement une classe de congruence modulo M .
- Déterminer le plus petit entier $n \geq 1$ tel que $4 \mid n$, $9 \mid n + 1$ et $25 \mid n + 2$.
- Soit $k \geq 2$. Montrer qu'il existe k entiers naturels consécutifs tous divisibles par un carré p^2 (p premier).
- Montrer qu'il existe k entiers naturels consécutifs dont aucun n'est de la forme p^α (p premier, $\alpha \in \mathbb{N}$).

Partie D • Corrigés

Des solutions détaillées, rédigées comme sur une copie

25 Corrigés du niveau I

■ Corrigé de l'exercice 1

1. Si $n = -3$: $n^2 + 1 = 10$ divise 0, donc $n = -3$ convient. Si $n \neq -3$: un diviseur d'un entier non nul lui est inférieur en valeur absolue, donc $n^2 + 1 \leq |n + 3| \leq |n| + 3$, soit $|n|^2 - |n| - 2 \leq 0$, c'est-à-dire $(|n| - 2)(|n| + 1) \leq 0$: $|n| \leq 2$. On teste : $n = -2$: $5 \nmid 1$; $n = -1$: $2 \nmid 2$; $n = 0$: $1 \nmid 3$; $n = 1$: $2 \nmid 4$; $n = 2$: $5 \nmid 5$. $S = \{-3, -1, 0, 1, 2\}$.
2. $n^2 + 7 = (n+1)(n-1) + 8$. Si $n+1 \mid n^2 + 7$, alors $n+1$ divise la combinaison $(n^2 + 7) - (n-1)(n+1) = 8$; réciproquement, si $n+1 \mid 8$, alors $n+1 \mid (n+1)(n-1) + 8$. Donc $n+1 \in \{1, 2, 4, 8\}$: $n \in \{0, 1, 3, 7\}$.
3. On cherche k tel que $5a + b \equiv k(2a + 3b) \pmod{13}$: $3k \equiv 1$ donne $k = 9$, et alors $2k = 18 \equiv 5 \checkmark$. Précisément, $5a + b = 9(2a + 3b) - 13(a + 2b)$: si $13 \mid 2a + 3b$, alors $13 \mid 5a + b$. Réciproquement, $2a + 3b = 3(5a + b) - 13a$: si $13 \mid 5a + b$, alors $13 \mid 2a + 3b$.
4. $x^2 = (y+1)^2 + 12 \iff (x-y-1)(x+y+1) = 12$. Comme $x+y+1 > 0$, on a $x-y-1 > 0$; la somme des deux facteurs, $2x$, est paire : ils ont même parité, donc sont pairs (12 n'est pas produit de deux impairs). Avec $x-y-1 \leq x+y+1$, la seule possibilité est 2×6 : $x-y-1 = 2$ et $x+y+1 = 6$, d'où $(x, y) = (4, 1)$ ($16 = 1 + 2 + 13 \checkmark$).

■ Corrigé de l'exercice 2

1. $1000 = 31 \times 32 + 8$ avec $0 \leq 8 < 31$: quotient 32, reste 8. $-1000 = 31 \times (-32) - 8 = 31 \times (-33) + 23$ avec $0 \leq 23 < 31$: quotient -33 , reste 23 (et non -8).
2. $a = 12q + 7$ ($q \in \mathbb{Z}$). Alors $a = 4(3q + 1) + 3$: reste 3 par 4 ; $a = 6(2q + 1) + 1$: reste 1 par 6 ; $a^2 = 144q^2 + 168q + 49 = 24(6q^2 + 7q + 2) + 1$: reste 1 par 24.
3. Un entier s'écrit $3q$, $3q+1$ ou $3q+2$; son carré vaut $3(3q^2)$, $3(3q^2 + 2q) + 1$ ou $3(3q^2 + 4q + 1) + 1$: le reste d'un carré par 3 est 0 ou 1. Or $(n-1)^2 + n^2 + (n+1)^2 = 3n^2 + 2$ a pour reste 2 : ce n'est **jamais un carré**.
4. $(2q)^2 = 4q^2$ et $(2q+1)^2 = 4(q^2 + q) + 1$: un carré a pour reste 0 ou 1 par 4. Or $(2a+1)^2 + (2b+1)^2 = 4(a^2 + a + b^2 + b) + 2$ a pour reste 2 : ce n'est **jamais un carré**.

■ Corrigé de l'exercice 3

1. a) $3^3 = 27 \equiv -1 \pmod{7}$, donc $3^6 \equiv 1$; $2026 = 6 \times 337 + 4$, d'où $3^{2026} = (3^6)^{337} 3^4 \equiv 81 \equiv 4 \pmod{7}$.
b) $5^2 \equiv 3$, $5^4 \equiv 9$, $5^5 \equiv 45 \equiv 1 \pmod{11}$; $2027 = 5 \times 405 + 2$: $5^{2027} \equiv 5^2 \equiv 3 \pmod{11}$.
c) $100 = 13 \times 7 + 9$, donc $100 \equiv 9 \pmod{13}$; $9^2 = 81 \equiv 3$ et $9^3 \equiv 27 \equiv 1 \pmod{13}$; $100 = 3 \times 33 + 1$: $100^{100} \equiv 9^{100} \equiv 9 \pmod{13}$: reste 9 .

2. a) $4 \times 7 = 28 \equiv 1 [9]$. En multipliant par 4 : $7x \equiv 4 \Rightarrow x \equiv 16 \equiv 7$; en multipliant par 7 : $x \equiv 7 \Rightarrow 7x \equiv 49 \equiv 4$. $x \equiv 7 [9]$.
- b) $6x \equiv 4 [10] \Leftrightarrow 10 \mid 6x - 4 \Leftrightarrow 5 \mid 3x - 2 \Leftrightarrow 3x \equiv 2 [5] \Leftrightarrow x \equiv 4 [5]$ (multiplier par 2, inverse de 3 modulo 5). $x \equiv 4 [5]$: on divise aussi le *module* par 2.
- c) Il suffit de tester $x \in \{0, \dots, 11\}$:

x	0	1	2	3	4	5	6	7	8	9	10	11
$x^2 + x \text{ modulo } 12$	0	2	6	0	8	6	6	8	0	6	2	0

$x \equiv 0, 3, 8 \text{ ou } 11 [12]$: quatre solutions pour une équation du second degré (car 12 n'est pas premier).

■ Corrigé de l'exercice 4

- Modulo 10 : $8^1, 8^2, 8^3, 8^4, 8^5 \equiv 8, 4, 2, 6, 8$. Comme $8^5 \equiv 8, 8^{n+4} \equiv 8^n$ pour $n \geq 1$; $2027 = 4 \times 506 + 3$: $8^{2027} \equiv 8^3 \equiv 2$. $2027 \equiv 7 [10]$ et $7^4 = 2401 \equiv 1 [10]$: $2027^{2027} \equiv 7^{2027} \equiv 7^3 = 343 \equiv 3 [10]$.
- $9^5 = 59049 \equiv 49 [100]$, donc $9^{10} \equiv 49^2 = 2401 \equiv 1 [100]$. Comme $2026 = 10 \times 202 + 6$: $9^{2026} \equiv 9^6 \equiv 49 \times 9 = 441 \equiv 41 [100]$: 9^{2026} se termine par 41 .
- Somme géométrique : $S = \frac{2^{2027}-1}{2-1} = 2^{2027} - 1$. Or $2^3 \equiv 1 [7]$ et $2027 = 3 \times 675 + 2$: $S \equiv 2^2 - 1 = 3 [7]$.
- $16 \equiv 3 [13]$, donc $4^{2n+1} = 4 \times 16^n \equiv 4 \times 3^n$, et $3^{n+2} = 9 \times 3^n$: la somme est congrue à $13 \times 3^n \equiv 0 [13]$.

■ Corrigé de l'exercice 5

- $88 = 8 \times 11$ avec $8 \wedge 11 = 1$: $N = \overline{2a3b6}$ est divisible par 88 si et seulement s'il l'est par 8 et par 11. Comme $1000 \equiv 0 [8]$, $N \equiv 3b6 = 306 + 10b \equiv 2 + 2b [8]$, et $8 \mid 2 + 2b \Leftrightarrow 4 \mid b + 1 \Leftrightarrow b \in \{3, 7\}$. Critère par 11 : $N \equiv 6 - b + 3 - a + 2 = 11 - a - b [11]$, donc $a + b \in \{0, 11\}$, soit $a + b = 11$ ($b \geq 3$). $N = 28336$ ou $N = 24376$ ($= 88 \times 322$ et 88×277).
- a) Divisions successives par 3 : $500 = 3 \times 166 + 2$, $166 = 3 \times 55 + 1$, $55 = 3 \times 18 + 1$, $18 = 3 \times 6 + 0$, $6 = 3 \times 2 + 0$, $2 = 3 \times 0 + 2$; on lit les restes de bas en haut : $500 = \overline{200112}^{(3)}$. Par 6 : $500 = 6 \times 83 + 2$, $83 = 6 \times 13 + 5$, $13 = 6 \times 2 + 1$, $2 = 6 \times 0 + 2$: $500 = \overline{2152}^{(6)}$.
b) $\overline{4E1}^{(16)} = 4 \times 16^2 + 14 \times 16 + 1 = 1024 + 224 + 1 = \overline{1249}$.
- Le chiffre 5 impose $b \geq 6$. $2b^2 + 5b + 3 = 2(b^2 + 2b + 5) \Leftrightarrow 5b + 3 = 4b + 10 \Leftrightarrow b = 7$
 $(\overline{253})^{(7)} = 136 = 2 \times 68 = 2 \times \overline{125}^{(7)}$ ✓).

■ Corrigé de l'exercice 6

- Algorithme d'Euclide (ligne 1 : quotients ; ligne 2 : dividendes puis diviseurs ; ligne 3 : restes) :

quotients	1	1	1	1	1	2
4389	2717	1672	1045	627	418	209
restes	1672	1045	627	418	209	0

Le dernier reste non nul est $4389 \wedge 2717 = 209$. Comme $4389 = 209 \times 21$ et $2717 = 209 \times 13$:

$$4389 \vee 2717 = 209 \times 21 \times 13 = \overline{57057} \quad (\text{et } 209 \times 57057 = 4389 \times 2717 \text{ ✓}), \quad \frac{2717}{4389} = \frac{13}{21}.$$

Les quotients valent presque tous 1 : 13 et 21 sont deux termes consécutifs de la suite de Fibonacci, cas où l'algorithme est le plus lent.

- $(2n + 1)^2 - 4(n^2 + n) = 1$: d'après le théorème de Bézout, $(n^2 + n) \wedge (2n + 1) = 1$.

3. Soient $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$ et $a' \leq b'$; alors $a \vee b = \frac{ab}{d} = da'b'$. L'équation devient $d(a'b' - 1) = 35$, donc $d \mid 35$.
 $d = 1$: $a'b' = 36$, d'où $(a', b') \in \{(1, 36), (4, 9)\} \cup \{(2, 18), (3, 12), (6, 6)\}$ ne sont pas premiers entre eux ; $d = 5$: $a'b' = 8$: $(1, 8)$; $d = 7$: $a'b' = 6$: $(1, 6), (2, 3)$; $d = 35$: $a'b' = 2$: $(1, 2)$.
 $(a, b) \in \{(1, 36), (4, 9), (5, 40), (7, 42), (14, 21), (35, 70)\}$.
4. Les conditions s'écrivent $n \equiv -1$ modulo 2, 3, 4, 5 et 6 : $n + 1$ est un multiple commun de 2, ..., 6, donc un multiple de leur PPCM 60. Avec $n + 1 \geq 1$, le plus petit est $n + 1 = 60$: $n = 59$.

■ Corrigé de l'exercice 7

1. Euclide : $2026 = 315 \times 6 + 136$, $315 = 136 \times 2 + 43$, $136 = 43 \times 3 + 7$, $43 = 7 \times 6 + 1$: $2026 \wedge 315 = 1$.
 On remonte :
 $1 = 43 - 6 \times 7 = 43 - 6(136 - 3 \times 43) = 19 \times 43 - 6 \times 136 = 19 \times 315 - 44 \times 136 = 283 \times 315 - 44 \times 2026$.
 D'où $(u, v) = (-44, 283)$.
2. $315 \times 283 = 1 + 44 \times 2026 \equiv 1 [2026]$: $w = 283$. En multipliant par 283 : $315x \equiv 5 \Rightarrow x \equiv 1415 [2026]$; en multipliant par 315 : $x \equiv 1415 \Rightarrow 315x \equiv 5 \times (315 \times 283) \equiv 5$. $x \equiv 1415 [2026]$.
3. Parmi $n, n + 1, n + 2, n + 3$, il y a deux entiers pairs consécutifs, dont l'un est multiple de 4 : le produit P est divisible par $2 \times 4 = 8$. L'un des trois premiers est multiple de 3 : $3 \mid P$. Comme $3 \wedge 8 = 1$, $24 \mid P$ (corollaire du théorème de Gauss).

■ Corrigé de l'exercice 8

1. $22^2 < 523 < 23^2$: il suffit de tester les premiers $p \leq 19$; les restes de 523 par 2, 3, 5, 7, 11, 13, 17, 19 sont 1, 1, 3, 5, 6, 3, 13, 10 : **523 est premier**. En testant les premiers, on trouve $527 = 17 \times 31$: 527 n'est pas premier.
2. $2016 = 2^5 \times 3^2 \times 7$ et $2025 = 3^4 \times 5^2$. $2016 \wedge 2025 = 3^2 = 9$; $2016 \vee 2025 = 2^5 \times 3^4 \times 5^2 \times 7 = 453600$.
 Nombres de diviseurs : $(5 + 1)(2 + 1)(1 + 1) = 36$ et $(4 + 1)(2 + 1) = 15$. Un diviseur pair de 2016 est $2^\alpha 3^\beta 7^\gamma$ avec $1 \leq \alpha \leq 5$: $5 \times 3 \times 2 = 30$ diviseurs pairs.
3. $n^2 - 8n + 15 = (n - 3)(n - 5)$. Si $|n - 3| \geq 2$ et $|n - 5| \geq 2$, ce produit (s'il est positif) admet le diviseur $|n - 3|$, avec $1 < |n - 3| < (n - 3)(n - 5)$: il n'est pas premier. Il faut donc $n - 3 = \pm 1$ ou $n - 5 = \pm 1$, soit $n \in \{2, 4, 6\}$: $n = 4$ donne -1 ; $n = 2$ et $n = 6$ donnent 3, premier. $n \in \{2, 6\}$.
4. Pour $2 \leq k \leq 2027$, k divise $2027!$, donc k divise $2027! + k$, avec $2 \leq k < 2027! + k$: $2027! + k$ est composé. On obtient 2026 entiers consécutifs composés.

26

Corrigés du niveau 2

■ Corrigé de l'exercice 9

1. a) $6^2 < 47 < 7^2$ et 47 n'est divisible ni par 2, ni par 3, ni par 5 : 47 est **premier**. b) 47 est premier et ne divise pas x : petit théorème de Fermat.
2. a) Si $47 \mid x$, alors $x^{17} \equiv 0 \not\equiv 3 [47]$: absurde. b) $17 \times 19 = 323 = 322 + 1 = 7 \times 46 + 1$ ✓. D'une part $x^{323} = (x^{17})^{19} \equiv 3^{19}$; d'autre part, avec 1.b, $x^{323} = (x^{46})^7 x \equiv x [47]$. Donc $x \equiv 3^{19} [47]$.
3. a) $3^5 = 243 = 5 \times 47 + 8$; $3^{10} \equiv 64 \equiv 17$; $3^4 = 81 \equiv -13 [47]$. Donc $3^{19} = 3^{10} \times 3^5 \times 3^4 \equiv 17 \times 8 \times (-13)$, avec $17 \times 8 = 136 \equiv -5$: $3^{19} \equiv 65 \equiv 18 [47]$.

b) $18^{17} \equiv (3^{19})^{17} = 3^{323} = (3^{46})^7 \times 3 \equiv 3 [47]$ (Fermat, $47 \nmid 3$). Ainsi : si $x^{17} \equiv 3$, alors $x \equiv 18$ (question 2) ; si $x \equiv 18$, alors $x^{17} \equiv 18^{17} \equiv 3$. $S = \{18 + 47k, k \in \mathbb{Z}\}$.

4. $47 \nmid 18$ et $2026 = 46 \times 44 + 2 : 18^{2026} \equiv 18^2 = 324 = 6 \times 47 + 42$. Le reste est $\boxed{42}$.

■ Corrigé de l'exercice 10

1. $391 = 255 \times 1 + 136$, $255 = 136 \times 1 + 119$, $136 = 119 \times 1 + 17$, $119 = 17 \times 7 : 391 \wedge 255 = \boxed{17}$. Comme $17 \mid 34$, (E) a des solutions ; avec $391 = 17 \times 23$, $255 = 17 \times 15$, $34 = 17 \times 2$, on divise par 17 : (E) $\Leftrightarrow 23x - 15y = 2$.

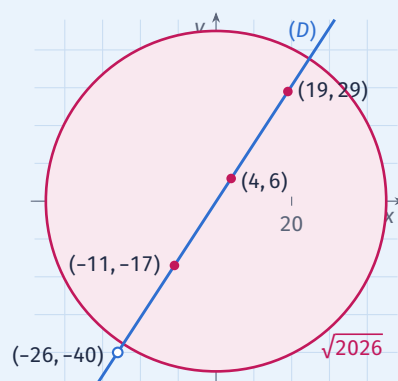
2. En multipliant par 2 : $23 \times 4 - 15 \times 6 = 2 : (4, 6)$ est solution. Alors (E') $\Leftrightarrow 23(x - 4) = 15(y - 6)$. Comme $15 \mid 23(x - 4)$ et $15 \wedge 23 = 1$, Gauss donne $x - 4 = 15k$ ($k \in \mathbb{Z}$), puis $23 \times 15k = 15(y - 6)$, soit $y = 6 + 23k$; réciproquement ces couples conviennent. $S = \{(4 + 15k, 6 + 23k), k \in \mathbb{Z}\}$.

3. $0 \leq 4 + 15k \leq 2026 \Leftrightarrow -\frac{4}{15} \leq k \leq \frac{2022}{15} \approx 134,8 \Leftrightarrow 0 \leq k \leq 134 : \boxed{135}$ solutions.

4. $f(k) = (4 + 15k)^2 + (6 + 23k)^2 = 754k^2 + 396k + 52$. On calcule $f(-1) = 410$, $f(0) = 52$, $f(1) = 1202$, tous < 2026 , et $f(-2) = 2276$, $f(2) = 3860$, tous deux ≥ 2026 . Le trinôme f ($754 > 0$) décroît puis croît : l'ensemble des réels t tels que $f(t) < 2026$ est un intervalle, qui contient -1 et 1 mais ni -2 ni 2 . Donc $k \in \{-1, 0, 1\}$:

$$(x, y) \in \{(-11, -17), (4, 6), (19, 29)\}.$$

Ce sont les **points à coordonnées entières de la droite** (D) : $23x - 15y = 2$ situés **dans le disque ouvert** de centre O et de rayon $\sqrt{2026} \approx 45$ (le point suivant, $(-26, -40)$, en est juste à l'extérieur : $OM \approx 47,7$).



■ Corrigé de l'exercice 11

1. $a = n(n^2 + 4n - 5) = \boxed{n(n-1)(n+5)}$ et $b = \boxed{(n-1)(3n+1)}$ (car $(n-1)(3n+1) = 3n^2 - 2n - 1 : n-1$ divise a et b).

2. a) $\beta - 3 \times n = 1$: par Bézout, $n \wedge \beta = 1$. Soient $\delta = \alpha \wedge \beta$ et $\delta' = (n+5) \wedge \beta$. Comme $n+5 \mid \alpha$, δ' divise α et β , donc $\delta' \mid \delta$. Réciproquement, $\delta \mid \beta$, donc $\delta \wedge n$ divise $\beta \wedge n = 1$; comme $\delta \mid n(n+5)$ et $\delta \wedge n = 1$, Gauss donne $\delta \mid n+5$, donc $\delta \mid \delta'$. Ainsi $\delta = \delta'$.

b) δ' divise $3(n+5) - (3n+1) = 14$.

c) Donc $\delta' \in \{1, 2, 7, 14\}$. D'une part $2 \mid \delta' \Leftrightarrow n+5$ et $3n+1$ pairs $\Leftrightarrow n$ impair. D'autre part $7 \mid \delta' \Leftrightarrow 7 \mid n+5$ (car alors 7 divise $3(n+5) - 14 = 3n+1$) $\Leftrightarrow n \equiv 2 [7]$. Modulo 14 :

$$(n+5) \wedge (3n+1) = \begin{cases} 14 & \text{si } n \equiv 9 [14] \\ 7 & \text{si } n \equiv 2 [14] \\ 2 & \text{si } n \text{ est impair et } n \not\equiv 9 [14] \\ 1 & \text{si } n \text{ est pair et } n \not\equiv 2 [14]. \end{cases}$$

3. $a = (n-1)\alpha$, $b = (n-1)\beta$ avec $n-1 \geq 1$, donc $a \wedge b = (n-1)(\alpha \wedge \beta) = \boxed{(n-1) \times ((n+5) \wedge (3n+1))}$, donné par le tableau ci-dessus. $2025 = 14 \times 144 + 9 : a \wedge b = 14 \times 2024 = \boxed{28336}$; $2027 \equiv 11 [14]$ est impair : $a \wedge b = 2 \times 2026 = \boxed{4052}$.

■ Corrigé de l'exercice 12

1. a) $85 - 84 = 1$ ✓. b) $85 = 6 \times 14 + 1 \equiv 1 [14]$ et $85 \equiv 0 [17]$; $84 \equiv 0 [14]$ et $84 = 85 - 1 \equiv -1 [17]$.
Donc $x_0 \equiv 9 \times 1 - 0 = 9 [14]$ et $x_0 \equiv 0 - 4 \times (-1) = 4 [17]$: x_0 est solution, et $x_0 = 765 - 336 = \boxed{429}$.
2. x est solution $\iff x \equiv x_0 [14]$ et $x \equiv x_0 [17] \iff 14 \mid x - x_0$ et $17 \mid x - x_0 \iff 238 \mid x - x_0$
(car $14 \wedge 17 = 1$) $\iff x \equiv 429 \equiv 191 [238]$ ($429 - 238 = 191$).
3. Le nombre N de billes est solution de (S) et $0 < N < 500$: $N \in \{191, 429\}$. Comme $191 = 5 \times 38 + 1$ et $429 = 5 \times 85 + 4$, seul 191 convient: $\boxed{191 \text{ billes}}$.

■ Corrigé de l'exercice 13

1. $x \equiv 0, \pm 1, \pm 2 [5]$ donne $x^2 \equiv 0, 1, 4 [5]$. Alors $2x^2 + 5y^2 \equiv 2x^2 \in \{0, 2, 8\}$, soit $\{0, 2, 3\}$ modulo 5, alors que $2026 \equiv 1 [5]$: **aucune solution**.
2. 2026 est pair et $x^2 - 3y^2 \equiv x^2 + y^2 \equiv x + y [2]$: x et y ont même parité. S'ils sont pairs, $x^2 - 3y^2 \equiv 0 [4]$, or $2026 \equiv 2 [4]$. S'ils sont impairs, $x^2 \equiv y^2 \equiv 1 [8]$ (un carré impair est $\equiv 1 [8]$), donc $x^2 - 3y^2 \equiv -2 \equiv 6 [8]$, or $2026 = 8 \times 253 + 2 \equiv 2 [8]$. **Aucune solution**.
3. On a bien $(n + 7)(n - 4) + 33 = n^2 + 3n - 28 + 33 = n^2 + 3n + 5$. Si $121 \mid n^2 + 3n + 5$, alors $11 \mid n^2 + 3n + 5$, et comme $11 \mid 33$: $11 \mid (n + 7)(n - 4)$, donc (lemme d'Euclide) $11 \mid n + 7$ ou $11 \mid n - 4$. Or $(n + 7) - (n - 4) = 11$: 11 divise les deux facteurs, donc $121 \mid (n + 7)(n - 4)$, puis $121 \mid 33$: absurde. 121 **ne divise jamais** $n^2 + 3n + 5$.
4. Modulo 7: $x \equiv 0, 1, 2, 3, 4, 5, 6$ donne $x^3 \equiv 0, 1, 1, 6, 1, 6, 6$. Si $7 \nmid x$, $x^3 \equiv \pm 1 [7]$. Alors $x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \in \{-3, -1, 1, 3\}$, et aucun de ces entiers n'est divisible par 7: $7 \nmid x^3 + y^3 + z^3$.

■ Corrigé de l'exercice 14

1. $b \equiv 1 [b - 1]$, donc $b^j \equiv 1$ et $N = \sum a_j b^j \equiv \sum a_j [b - 1]$. De même $b \equiv -1 [b + 1]$, donc $b^j \equiv (-1)^j$ et $N \equiv \sum (-1)^j a_j [b + 1]$.
2. $6 + 2 + 4 + 1 + 5 = 18 \equiv 0 [6]$: **divisible par 6**. $5 - 1 + 4 - 2 + 6 = 12 \equiv 4 [8]$: **non divisible par 8** (reste 4). (En effet $\overline{62415}^{(7)} = 15300 = 6 \times 2550 = 8 \times 1912 + 4$.)
3. Ici $x \in \{0, \dots, 8\}$. Modulo 8: $N \equiv 3 + x + 5 + x + 2 = 2x + 10$, et $8 \mid 2x + 10 \iff 4 \mid x + 5 \iff \boxed{x \in \{3, 7\}}$.
Modulo 10: $N \equiv 2 - x + 5 - x + 3 = 10 - 2x$, et $10 \mid 2x \iff 5 \mid x \iff \boxed{x \in \{0, 5\}}$ (aucun chiffre ne convient pour les deux).
4. a) 2026 a trois chiffres en base $b \iff b^2 \leq 2026 < b^3$. Or $12^3 = 1728 \leq 2026 < 2197 = 13^3$ et $45^2 = 2025 \leq 2026 < 2116 = 46^2$: $\boxed{13 \leq b \leq 45}$, soit 33 bases.
b) $2026 = \overline{101}^{(b)} \iff b^2 + 1 = 2026 \iff b^2 = 2025 \iff \boxed{b = 45}$ (les chiffres 0 et 1 sont bien < 45).

■ Corrigé de l'exercice 15

1. 17 est premier et ne divise ni 3 ni 5: $3^{16} \equiv 5^{16} \equiv 1 [17]$; $2026 = 16 \times 126 + 10$. Puis $3^4 = 81 \equiv -4$, $3^8 \equiv 16 \equiv -1$, $3^{10} \equiv -9$; et $5^2 \equiv 8$, $5^4 \equiv 64 \equiv -4$, $5^8 \equiv -1$, $5^{10} \equiv -8$. Donc $3^{2026} + 5^{2026} \equiv -9 - 8 = -17 \equiv 0 [17]$.
2. a) Si $p \mid n$, $n^{13} \equiv 0 \equiv n$. Sinon, Fermat: $n^{p-1} \equiv 1$; avec $12 = (p - 1)t$, $n^{12} \equiv 1$, donc $n^{13} \equiv n [p]$.
b) Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12; $p = d + 1$ premier donne $p \in \{2, 3, 5, 7, 13\}$. Ces cinq nombres premiers distincts divisent $n^{13} - n$; étant premiers entre eux deux à deux, leur produit $2 \times 3 \times 5 \times 7 \times 13 = \boxed{2730}$ divise $n^{13} - n$.

3. $R = \underbrace{11 \dots 1}_{p-1} = \frac{10^{p-1}-1}{9}$. Comme $p \neq 2, 5$, $p \nmid 10$ et $10^{p-1} \equiv 1 [p]$: $p \mid 9R$. Comme $p \neq 3$, $p \wedge 9 = 1$ et Gauss donne $p \mid R$.
4. Pour $1 \leq k \leq p-1$, $p \nmid k$, donc $k^{p-1} \equiv 1 [p]$: la somme est congrue à $p-1 \equiv -1 [p]$.

■ Corrigé de l'exercice 16

1. $u_0 = 1 = 2^2 - 3$; si $u_n = 2^{n+2} - 3$, alors $u_{n+1} = 2(2^{n+2} - 3) + 3 = 2^{n+3} - 3$: par récurrence, $u_n = 2^{n+2} - 3$.
Soit $d = u_n \wedge u_{n+1}$: d divise $u_{n+1} - 2u_n = 3$, donc $d \in \{1, 3\}$; or $u_n \equiv 2^{n+2} \not\equiv 0 [3]$ (3 premier ne divise pas 2^{n+2}). Donc $u_n \wedge u_{n+1} = 1$.
2. a) $5 \mid u_n \iff 2^{n+2} \equiv 3 [5]$. Les puissances $2^1, 2^2, 2^3, 2^4$ valent 2, 4, 3, 1 modulo 5 (période 4) : $2^k \equiv 3 \iff k \equiv 3 [4]$. D'où $5 \mid u_n \iff n \equiv 1 [4]$ (ex. $u_1 = 5$).
Modulo 13, $2^1, \dots, 2^{12}$ valent 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1 (période 12) : $2^k \equiv 3 \iff k \equiv 4 [12]$, d'où $13 \mid u_n \iff n \equiv 2 [12]$ (ex. $u_2 = 13$).
- b) Comme $5 \wedge 13 = 1$: $65 \mid u_n \iff n \equiv 1 [4]$ et $n \equiv 2 [12]$. Mais $n \equiv 2 [12]$ entraîne $n \equiv 2 [4]$: c'est **impossible**, 65 ne divise aucun u_n .
3. Modulo 10, $2^k \equiv 2, 4, 8, 6$ selon que $k \equiv 1, 2, 3, 0 [4]$ ($k \geq 1$). Or $u_{2026} = 2^{2028} - 3$ et $2028 \equiv 0 [4]$: 2^{2028} se termine par 6, et u_{2026} par $\boxed{3}$.

27

Corrigés du niveau 3

■ Corrigé de l'exercice 17

1. $(\alpha_1 + 1) \dots (\alpha_k + 1) = 2026 = 2 \times 1013$ avec des facteurs ≥ 2 et 1013 premier : soit $k = 1$ et $n = p^{2025} \geq 2^{2025}$; soit $k = 2$ et $n = p^{1012} q$ ($p \neq q$ premiers). Dans ce cas, si $p = 2$, $n \geq 3 \times 2^{1012}$; si $p \geq 3$, $n \geq 3^{1012} = 3 \times 3^{1011} > 3 \times 2^{1012}$ car $(\frac{3}{2})^{1011} > 2$. Enfin $3 \times 2^{1012} < 2^{1014} < 2^{2025}$. $n = 3 \times 2^{1012}$.
2. Si $ab = n$ et $a \wedge b = 1$, chaque p_i divise a ou b mais pas les deux ; comme $v_{p_i}(a) + v_{p_i}(b) = \alpha_i$, le facteur $p_i^{\alpha_i}$ est entièrement dans a ou entièrement dans b . Donc $a = \prod_{i \in I} p_i^{\alpha_i}$ pour une partie I de $\{1, \dots, k\}$, et $b = \frac{n}{a}$; réciproquement chaque partie I donne un couple qui convient. Il y a $\boxed{2^k}$ couples.
3. Si $a \vee b = n$, alors $a \mid n$ et $b \mid n$: $a = \prod p_i^{\beta_i}$, $b = \prod p_i^{\gamma_i}$ avec $0 \leq \beta_i, \gamma_i \leq \alpha_i$. Un multiple commun m de a et b vérifie $v_{p_i}(m) \geq \max(\beta_i, \gamma_i)$, et $\prod p_i^{\max(\beta_i, \gamma_i)}$ est un multiple commun : $a \vee b = \prod p_i^{\max(\beta_i, \gamma_i)}$.
Donc $a \vee b = n \iff \max(\beta_i, \gamma_i) = \alpha_i$ pour tout i . Pour chaque i , parmi les $(\alpha_i + 1)^2$ couples (β_i, γ_i) , α_i^2 ont leurs deux termes $< \alpha_i$: il en reste $2\alpha_i + 1$. D'où $(2\alpha_1 + 1) \dots (2\alpha_k + 1)$ couples.
 $360 = 2^3 \times 3^2 \times 5 : 7 \times 5 \times 3 = \boxed{105}$ couples.

■ Corrigé de l'exercice 18

1. $2^p - 1$ est impair, donc q aussi, et $2^p \equiv 1 [q]$. L'ordre k de 2 modulo q divise p , donc $k \in \{1, p\}$; $k = 1$ donnerait $q \mid 1$. Donc $k = p$, et $p \mid q - 1$. Comme $q - 1$ est pair et $p \wedge 2 = 1$ (p impair) : $\boxed{2p \mid q - 1}$. (Exemple du cours : $2^{11} - 1 = 23 \times 89$, et $23 = 1 + 22$, $89 = 1 + 4 \times 22$.)
2. Si 8191 était composé, il aurait un diviseur premier $q \leq \sqrt{8191} < 91$, avec $q \equiv 1 [26]$: $q \in \{27, 53, 79\}$, et 27 n'est pas premier. Or $8191 = 53 \times 154 + 29 = 79 \times 103 + 54$: $\boxed{8191 \text{ est premier}}$.

3. $n^4 \equiv -1 [q]$, donc $n^8 \equiv 1$; $q \nmid n$ (sinon $n^4 + 1 \equiv 1$). L'ordre k de n modulo q divise 8 : $k \in \{1, 2, 4, 8\}$. Si $k \mid 4$, alors $n^4 \equiv 1$, d'où $-1 \equiv 1$ et $q \mid 2$: exclu. Donc $k = 8$, et $k \mid q - 1$: $q \equiv 1 [8]$.
4. 10001 est impair ; s'il est composé, il a un diviseur premier $q \leq \sqrt{10001} < 101$, avec $q \equiv 1 [8]$: $q \in \{17, 41, 73, 89, 97\}$. On trouve $10001 = 17 \times 588 + 5 = 41 \times 243 + 38 = 73 \times 137$, et 137 est premier (non divisible par 2, 3, 5, 7, 11, et $12^2 > 137$) : $10001 = 73 \times 137$ (avec bien $73 \equiv 137 \equiv 1 [8]$).

■ Corrigé de l'exercice 19

1. a) $4x = 2 - 7 = -5 = \bar{6}$; comme $4 \times 3 = 12 = \bar{1}$, $x = 3 \times \bar{6} = \bar{18} = \bar{7}$.
 b) $y = 2x - 4$, puis $3x + 5(2x - 4) = \bar{1} \iff 13x = \bar{21} \iff 2x = \bar{10} \iff x = \bar{5}$ ($\bar{2}$ est inversible, d'inverse $\bar{6}$), et $y = \bar{10} - 4 = \bar{6}$: $(x, y) = (\bar{5}, \bar{6})$ ($\bar{15} + \bar{30} = \bar{45} = \bar{1}$ ✓).
 c) Les carrés de $\bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \pm\bar{4}, \pm\bar{5}$ sont $\bar{0}, \bar{1}, \bar{4}, \bar{9}, \bar{5}, \bar{3}$: $x^2 = \bar{5} \iff x \in \{\bar{4}, \bar{7}\}$.
2. a) $\bar{a}$ est inversible $\iff a \wedge 12 = 1$: $\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$; et $\bar{5}^2 = \bar{25} = \bar{1}$, $\bar{7}^2 = \bar{49} = \bar{1}$, $\bar{11}^2 = \bar{121} = \bar{1}$: **chacun est son propre inverse**.
 b) $4x = \bar{8} \iff 12 \mid 4x - 8 \iff 3 \mid x - 2 \iff x \in \{\bar{2}, \bar{5}, \bar{8}, \bar{11}\}$. c) $12 \mid 3x - 5$ entraînerait $3 \mid 5$: aucune solution.
 d) Si $x^2 = \bar{1}$, x est inversible (d'inverse x), donc $x \in \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$, et ces quatre classes conviennent (a) : **quatre solutions**.
3. $x^2 = \bar{1} \iff (x - \bar{1})(x + \bar{1}) = \bar{0}$. Si $x = \bar{a}$: $p \mid (a - 1)(a + 1)$, donc (lemme d'Euclide) $p \mid a - 1$ ou $p \mid a + 1$, soit $x = \bar{1}$ ou $x = \bar{-1}$. Dans $\mathbb{Z}/12\mathbb{Z}$, il y a plus de solutions car un produit peut être nul sans qu'un facteur le soit (pour $x = \bar{5}$: $(x - \bar{1})(x + \bar{1}) = \bar{4} \times \bar{6} = \bar{0}$).

■ Corrigé de l'exercice 20

1. $p \mid x^2 - y^2 = (x - y)(x + y) \iff p \mid x - y$ ou $p \mid x + y$ (lemme d'Euclide). Tout reste non nul est congru à $\pm r$ avec $1 \leq r \leq \frac{p-1}{2}$, donc les carrés non nuls sont les restes de $1^2, \dots, \left(\frac{p-1}{2}\right)^2$; ils sont distincts : si $i^2 \equiv j^2$ avec $1 \leq i < j \leq \frac{p-1}{2}$, alors $p \mid j - i$ ou $p \mid i + j$, avec $0 < j - i < i + j < p$, absurde. Il y en a $\frac{p-1}{2}$. Pour $p = 13$: 1, 4, 9, 16, 25, 36 donnent $\{1, 3, 4, 9, 10, 12\}$.
2. $p \nmid a$ entraîne $p \nmid x$, et Fermat donne $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 [p]$. Si $p \equiv 3 [4]$, $\frac{p-1}{2}$ est impair et $(-1)^{\frac{p-1}{2}} = -1 \not\equiv 1 [p]$ ($p \neq 2$) : **-1 n'est pas un carré modulo p** . Enfin $3^5 = 243 = 7 \times 31 + 26 \equiv -5$, donc $3^{15} \equiv -125 = -4 \times 31 - 1 \equiv -1 \not\equiv 1 [31]$: **3 n'est pas un carré modulo 31**.
3. $4m^2 + 1$ est impair, donc q aussi, et $(2m)^2 \equiv -1 [q]$: -1 est un carré modulo q , donc $q \not\equiv 3 [4]$ (question 2) : $q \equiv 1 [4]$. Si $p_1, \dots, p_r$ étaient tous les premiers de la forme $4k + 1$ (il y en a : 5), l'entier $N = 4(p_1 \cdots p_r)^2 + 1 \geq 5$ aurait un diviseur premier $q \equiv 1 [4]$, donc $q = p_i$ pour un i , et $p_i \mid N - 4(p_1 \cdots p_r)^2 = 1$: absurde. Il y a **une infinité** de premiers $4k + 1$.

■ Corrigé de l'exercice 21

1. En multipliant les décompositions $|a| = \prod p^{v_p(a)}$ et $|b| = \prod p^{v_p(b)}$, on obtient $|ab| = \prod p^{v_p(a) + v_p(b)}$; par unicité de la décomposition, $v_p(ab) = v_p(a) + v_p(b)$. Si $b = ac$ ($c \in \mathbb{N}^*$), alors $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$. Réciproquement, si $v_p(a) \leq v_p(b)$ pour tout p , l'entier $c = \prod p^{v_p(b) - v_p(a)}$ vérifie $ac = b$.

2. $n v_p(a) = v_p(a^n) \leq v_p(b^n) = n v_p(b)$, donc $v_p(a) \leq v_p(b)$ pour tout p , et $a \mid b$. Si $\sqrt[3]{2026} = \frac{u}{v}$ ($u, v \in \mathbb{N}^*$), alors $u^3 = 2026v^3$, donc $v^3 \mid u^3$, $v \mid u$ et $\sqrt[3]{2026} \in \mathbb{N}$; or $12^3 = 1728 < 2026 < 2197 = 13^3$: absurde. $\sqrt[3]{2026}$ est **irrationnel**.
3. Si $p \mid a$, alors $p \nmid b$ ($a \wedge b = 1$) et $v_p(a) = v_p(ab) = v_p(c^n) = n v_p(c)$. Tous les exposants de a sont des multiples de n : $a = s^n$ avec $s = \prod_{p \mid a} p^{v_p(a)/n}$ (et $a = 1 = 1^n$ si $a = 1$). De même pour b .
4. $(n+1) - n = 1$: $n \wedge (n+1) = 1$. Si $n(n+1) = c^2$, alors (3.) $n = s^2$, $n+1 = t^2$, et $(t-s)(t+s) = 1$ impose $s = 0$, soit $n = 0$: exclu. Ensuite $n+1$ est premier avec n et avec $n+2$, donc avec $n(n+2)$. Si $n(n+1)(n+2) = c^2$, alors $n+1 = t^2$ et $n(n+2) = (n+1)^2 - 1 = t^4 - 1 = s^2$, avec $t \geq 2$. Mais $(t^2 - 1)^2 = t^4 - 2t^2 + 1 < t^4 - 1 < (t^2)^2$: s^2 serait strictement entre deux carrés consécutifs, absurde.

■ Corrigé de l'exercice 22

1. Ils ne sont pas tous deux pairs ($x \wedge y = 1$). S'ils étaient tous deux impairs, $z^2 = x^2 + y^2 \equiv 2 \pmod{4}$, alors qu'un carré est $\equiv 0$ ou $1 \pmod{4}$.
2. x impair et y pair, donc z^2 et z sont impairs. Un premier ℓ divisant x et z diviserait $z^2 - x^2 = y^2$, donc y (lemme d'Euclide) : exclu, donc $x \wedge z = 1$. Les entiers $u = \frac{z+x}{2}$ et $v = \frac{z-x}{2}$ sont dans $\mathbb{N}^*$ ($z > x$) ; $d = u \wedge v$ divise $u+v = z$ et $u-v = x$, donc $d = 1$. Et $uv = \frac{z^2 - x^2}{4} = \left(\frac{y}{2}\right)^2$. Par l'exercice 21 (3.) : $u = m^2$, $v = n^2$ ($m, n \in \mathbb{N}^*$). Alors $z = u+v = m^2 + n^2$, $x = u-v = m^2 - n^2$ (donc $m > n$), et $\left(\frac{y}{2}\right)^2 = m^2 n^2$, soit $y = 2mn$. Un diviseur commun de m et n divise u et v : $m \wedge n = 1$; enfin $x = m^2 - n^2$ impair impose des parités différentes.
3. $(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2 n^2 + n^4 = (m^2 + n^2)^2$, et $x, y, z \in \mathbb{N}^*$ car $m > n \geq 1$. Si un premier ℓ divisait x et y : x est impair, donc $\ell \neq 2$ et $\ell \mid m$ ou $\ell \mid n$; si $\ell \mid m$, alors $\ell \mid m^2 - x = n^2$, donc $\ell \mid n$: contredit $m \wedge n = 1$ (de même si $\ell \mid n$). Le triplet est **primitif**.
4. Soit $\delta = x \wedge y$: $\delta^2 \mid x^2 + y^2 = 65^2$, donc $\delta \mid 65$ (exercice 21), et $\left(\frac{x}{\delta}, \frac{y}{\delta}, \frac{65}{\delta}\right)$ est primitif, d'hypoténuse $z' = m^2 + n^2 \in \{65, 13, 5\}$ ($z' = 1$ est impossible). Avec $m > n \geq 1$: $65 = 8^2 + 1^2 = 7^2 + 4^2$ (seuls $m \in \{6, 7, 8\}$ sont possibles, et $65 - 36 = 29$ n'est pas un carré) ; $13 = 3^2 + 2^2$; $5 = 2^2 + 1^2$. On obtient $(63, 16)$, $(33, 56)$ (primitifs), $13 \times (3, 4) = (39, 52)$ et $5 \times (5, 12) = (25, 60)$.
 $\boxed{\{x, y\} \in \{\{16, 63\}, \{33, 56\}, \{39, 52\}, \{25, 60\}\}}$: 8 couples ordonnés.

■ Corrigé de l'exercice 23

1. Un carré est $\equiv 0$ ou $1 \pmod{4}$, donc $x^2 - y^2 \equiv 0, 1$ ou $3 \pmod{4}$, alors que $2026 \equiv 2 \pmod{4}$: **aucune solution**. Pour 2027 : $(x-y)(x+y) = 2027$ avec $x+y > 0$, donc $0 < x-y \leq x+y$; 2027 étant premier, $x-y = 1$ et $x+y = 2027$: $\boxed{(x, y) = (1014, 1013)}$.
2. Soit $S_n = 1! + \dots + n!$: $S_1 = 1 = 1^2$, $S_2 = 3$, $S_3 = 9 = 3^2$, $S_4 = 33$. Pour $k \geq 5$, $5 \mid k!$, donc pour $n \geq 4$: $S_n \equiv 33 \equiv 3 \pmod{5}$, alors qu'un carré est $\equiv 0, 1$ ou $4 \pmod{5}$; et $S_2 = 3$ n'est pas un carré.
 $\boxed{(n, m) \in \{(1, 1), (3, 3)\}}$.
3. $x = 0$: 8 ; $x = 1$: 9 = $(\pm 3)^2$; $x = 2$: 11. Pour $x \geq 3$: $2^x + 7 \equiv 7 \pmod{8}$, or un carré est $\equiv 0, 1$ ou $4 \pmod{8}$.
 $\boxed{S = \{(1, 3), (1, -3)\}}$.

28

Corrigés du niveau 4**■ Corrigé de l'exercice 24**

1. a) $2^n - 1$ est impair et n le divise : n , donc p , est impair. $2^n \equiv 1 [p]$ donne $k \mid n$; Fermat ($p \nmid 2$) donne $2^{p-1} \equiv 1$, donc $k \mid p - 1$.
b) Si $k \geq 2$, un diviseur premier r de k divise n et vérifie $r \leq k \leq p - 1 < p$: cela contredit la minimalité de p . Donc $k = 1$ et $p \mid 2^1 - 1 = 1$: absurde. Aucun $n \geq 2$ ne convient, et $n = 1$ convient : $\boxed{n = 1}$.
2. $2 \equiv -1 [3]$, donc $n \cdot 2^n + 1 \equiv (-1)^n n + 1 [3]$. Si n est pair : il faut $n \equiv -1 \equiv 2 [3]$; si n est impair : $n \equiv 1 [3]$. En combinant parité et reste modulo 3 : $\boxed{n \equiv 1 \text{ ou } 2 [6]}$.
3. $p \nmid 2$, donc $2^{p-1} \equiv 1$ et $2^n = (2^{p-1})^{mp+1} \equiv 1 [p]$; et $n = (p-1)(mp+1) \equiv (-1) \times 1 = -1 [p]$. Donc $n \cdot 2^n + 1 \equiv -1 + 1 = 0 [p]$. Les entiers $(p-1)(mp+1)$, $m \in \mathbb{N}$, sont deux à deux distincts : **une infinité** de n conviennent. (Pour $p = 3$: $n = 6m + 2$, en accord avec 2.)

■ Corrigé de l'exercice 25

1. Si x est pair, $x^3 \equiv 0 [8]$ et $y^2 \equiv 7 [8]$; or un carré est $\equiv 0, 1$ ou $4 [8]$. Donc x est impair.
2. $(x+2)(x^2-2x+4) = x^3+8 = y^2+1$ ✓. Avec $x-1 = 2t$: $x^2-2x+4 = (x-1)^2+3 = 4t^2+3 \equiv 3 [4]$.
3. $M = x^2-2x+4 \geq 3$ est impair ; si tous ses facteurs premiers (impairs) étaient $\equiv 1 [4]$, leur produit M serait $\equiv 1 [4]$. Donc un premier $q \equiv 3 [4]$ divise M , donc $y^2+1 : y^2 \equiv -1 [q]$, et -1 serait un carré modulo le premier $q \equiv 3 [4]$, ce qui contredit l'exercice 20 (2.). L'équation $y^2 = x^3+7$ n'a **aucune solution** dans $\mathbb{Z}^2$.
L'idée : ajouter 1 aux deux membres pour faire apparaître x^3+2^3 , qui se factorise.

■ Corrigé de l'exercice 26

1. $(a^2+2b^2)^2 - (2ab)^2 = a^4+4a^2b^2+4b^4-4a^2b^2 = a^4+4b^4$.
2. Avec $b = 1$: $n^4+4 = (n^2+2n+2)(n^2-2n+2)$, où $n^2-2n+2 = (n-1)^2+1 \geq 1$, avec égalité si et seulement si $n = 1$. Pour $n \geq 2$, les deux facteurs sont ≥ 2 : n^4+4 est composé ; pour $n = 1, 5$ est premier. Avec $b = 2$: $n^4+64 = (n^2+4n+8)(n^2-4n+8)$, où $n^2-4n+8 = (n-2)^2+4 \geq 4$ et $n^2+4n+8 \geq 13$: **jamais premier**.
3. $n = 1$: 5, premier. Si $n \geq 2$ est pair, n^4+4^n est pair et > 2 : composé. Si $n = 2k+1$ avec $k \geq 1$: $4^n = 4(2^k)^4$, et la question 1 avec $a = n$, $b = 2^k$ donne deux facteurs, le plus petit étant $n^2+2^{2k+1} - n2^{k+1} = (n-2^k)^2+2^{2k} \geq 4$: composé. Comme $2027 = 2 \times 1013 + 1$, 2027^4+4^{2027} est **composé**.

■ Corrigé de l'exercice 27

1. $e \wedge M = 1$: par Bézout, $eu + Mv = 1$ avec $u, v \in \mathbb{Z}$, donc $eu \equiv 1 [M]$; $d = u + tM$, avec $t \in \mathbb{N}$ assez grand pour que $d \geq 1$, vérifie encore $ed \equiv 1 [M]$.
2. $ed \geq 1$ et $ed \equiv 1 [M]$: $ed = 1 + hM$ avec $h \in \mathbb{N}$. Si $p \mid x$: $x^{ed} \equiv 0 \equiv x [p]$. Sinon, Fermat : $x^{ed} = x(x^{p-1})^{h(q-1)} \equiv x [p]$. De même $x^{ed} \equiv x [q]$. Ainsi p et q , premiers entre eux, divisent $x^{ed} - x$: $pq = N$ le divise.

3. a) $N = \boxed{55}$, $M = 4 \times 10 = \boxed{40}$; $7 \times 23 = 161 = 4 \times 40 + 1$: $\boxed{d = 23}$ (unique dans $\{1, \dots, 40\}$, car 7 est inversible modulo 40).
 b) $13^2 = 169 \equiv 4$, $13^4 \equiv 16$, $13^7 = 13^4 \times 13^2 \times 13 \equiv 16 \times 4 \times 13 = 832 = 15 \times 55 + 7$: $\boxed{y = 7}$. Puis $7^2 \equiv -6$, $7^4 \equiv 36$, $7^8 \equiv 1296 \equiv 31$, $7^{16} \equiv 961 \equiv 26 \pmod{55}$; $7^{23} = 7^{16} \times 7^4 \times 7^2 \times 7 \equiv 26 \times 36 \times (-6) \times 7$, avec $26 \times 36 = 936 = 17 \times 55 + 1$: $7^{23} \equiv -42 \equiv \boxed{13} \pmod{55}$ ✓.

Pour calculer d , il faut connaître M , donc factoriser N : facile ici, pratiquement impossible pour un N de plusieurs centaines de chiffres.

■ Corrigé de l'exercice 28

- a) Soit $t = a - 1$, avec $p \mid t$. Récurrence : $a^0 = 1$; si $a^j \equiv 1 + jt \pmod{p^2}$, alors $a^{j+1} \equiv (1 + jt)(1 + t) = 1 + (j + 1)t + jt^2 \equiv 1 + (j + 1)t$, car $p^2 \mid t^2$.
 b) $S = \sum_{j=0}^{p-1} a^j \equiv \sum_{j=0}^{p-1} (1 + jt) = p + t \frac{p(p-1)}{2} \pmod{p^2}$; p étant impair, $\frac{p-1}{2} \in \mathbb{N}$, et $p \mid t$: $p^2 \mid t p \frac{p-1}{2}$. Donc $S \equiv p \pmod{p^2}$: $v_p(S) = 1$. Comme $a^p - 1 = (a - 1)S$: $v_p(a^p - 1) = v_p(a - 1) + 1$.
 c) Récurrence sur j ($j = 0$: évident). Si $v_p(a^{p^j} - 1) = v_p(a - 1) + j \geq 1$, alors $c = a^{p^j}$ vérifie $c \equiv 1 \pmod{p}$ et $c \neq 1$ (car $|a| \geq 2$: $a \equiv 1$, $a \neq 1$, et $a \neq -1$ puisque $p \neq 2$); b) appliqué à c donne $v_p(a^{p^{j+1}} - 1) = v_p(c - 1) + 1 = v_p(a - 1) + j + 1$.
- $a = 16 \equiv 1 \pmod{5}$, $a \neq 1$, et $v_5(a - 1) = v_5(15) = 1$. Comme $16^{5^j} = 2^{4 \cdot 5^j}$, 1.c donne $\boxed{v_5(2^{4 \cdot 5^j} - 1) = j + 1}$.
- a) Par 2. ($j = k - 1$): $5^k \mid 2^{4 \cdot 5^{k-1}} - 1$. Et $2^{2 \cdot 5^{k-1}} = 4^{5^{k-1}} \equiv (-1)^{5^{k-1}} = -1 \pmod{5}$, car 5^{k-1} est impair.
 b) Division euclidienne $4 \cdot 5^{k-1} = \omega s + r$, $0 \leq r < \omega$: $2^r \equiv 1$, donc $r = 0$ et $\omega \mid 4 \cdot 5^{k-1}$: $\omega = 2^e 5^j$ avec $e \leq 2$, $j \leq k - 1$. Si $e \leq 1$, $\omega \mid 2 \cdot 5^{k-1}$, donc $2^{2 \cdot 5^{k-1}} \equiv 1 \pmod{5^k}$, et a fortiori modulo 5: contredit a). Donc $\omega = 4 \cdot 5^j$, et $16^{5^j} \equiv 1 \pmod{5^k}$; par 1.c, $v_5(16^{5^j} - 1) = 1 + j \geq k$, d'où $j = k - 1$: $\boxed{\omega = 4 \cdot 5^{k-1}}$ (pour $k = 4$: $2^{500} \equiv 1 \pmod{625}$, et 500 est le plus petit exposant).
 c) Les restes de $2^0, 2^1, \dots, 2^{\omega-1}$ modulo 5^k sont distincts: si $2^i \equiv 2^j$ avec $0 \leq i < j < \omega$, alors $2^{j-i} \equiv 1 \pmod{5^k}$ (2 est inversible modulo 5^k), avec $0 < j - i < \omega$: absurde. Ce sont $4 \cdot 5^{k-1}$ restes non divisibles par 5; or $\{0, \dots, 5^k - 1\}$ en contient exactement $5^k - 5^{k-1} = 4 \cdot 5^{k-1}$: ce sont tous. Tout entier non divisible par 5 est donc congru modulo 5^k à une puissance de 2.

■ Corrigé de l'exercice 29

- $\sum_{j=0}^{2m+1} C_{2m+1}^j = (1 + 1)^{2m+1} = 2^{2m+1}$. Cette somme contient les deux termes égaux C_{2m+1}^m et C_{2m+1}^{m+1} , donc $2 C_{2m+1}^m \leq 2^{2m+1}$: $C_{2m+1}^m \leq 4^m$.
- $C_{2m+1}^m \times m!(m + 1)! = (2m + 1)!$. Comme $p \leq 2m + 1$, $p \mid (2m + 1)!$; comme $p > m + 1$, p ne divise aucun facteur de $m!(m + 1)!$, donc (lemme d'Euclide) $p \wedge m!(m + 1)! = 1$, et Gauss donne $p \mid C_{2m+1}^m$. Les premiers de $[m + 2, 2m + 1]$, distincts, divisent tous C_{2m+1}^m , donc leur produit $\frac{P(2m+1)}{P(m+1)}$ le divise aussi: $\frac{P(2m+1)}{P(m+1)} \leq C_{2m+1}^m \leq 4^m$.
- $P(2) = 2 < 16$. Soit $n \geq 3$; on suppose $P(j) < 4^j$ pour $2 \leq j < n$. Si n est pair, il n'est pas premier ($n \geq 4$): $P(n) = P(n - 1) < 4^{n-1} < 4^n$. Si $n = 2m + 1$ ($m \geq 1$), alors $2 \leq m + 1 < n$ et, par 2.: $P(n) \leq 4^m P(m + 1) < 4^m \times 4^{m+1} = 4^n$. Donc $\boxed{P(n) < 4^n}$ pour tout $n \geq 2$.
 Exemple: $P(30) = 6\,469\,693\,230 \approx 6,5 \times 10^9$, très loin de $4^{30} \approx 1,15 \times 10^{18}$.

■ **Corrigé de l'exercice 30**

- $2^n + 1$ est impair et n le divise : n et p sont impairs. $p \mid 2^n + 1$ donne $2^n \equiv -1$, donc $2^{2n} \equiv 1 \pmod{p}$: $k \mid 2n$, et $k \mid p - 1$ (Fermat). Les facteurs premiers de $p - 1$ sont $< p$, ceux de n sont $\geq p$: $(p - 1) \wedge n = 1$, donc $k \wedge n = 1$, et Gauss ($k \mid 2n$) donne $k \mid 2$. Alors $2^2 \equiv 1 \pmod{p}$, $p \mid 3$: $p = 3$.
- a) n impair, donc m impair. $2^m \equiv (-1)^m = -1 \pmod{3}$: $3 \mid 2^m + 1$. Modulo 9, $2^6 = 64 \equiv 1$; m impair et non multiple de 3 donne $m \equiv 1$ ou $5 \pmod{6}$, donc $2^m \equiv 2$ ou $2^5 \equiv 5 \pmod{9}$, et $2^m + 1 \equiv 3$ ou $6 \pmod{9}$: $v_3(2^m + 1) = 1$.
b) $a = (-2)^m = -2^m \equiv 1 \pmod{3}$, $a \neq 1$ et $v_3(a - 1) = v_3(2^m + 1) = 1$. Par 28.1.c : $v_3(a^{3^j} - 1) = 1 + j$; or $a^{3^j} = (-2)^n = -2^n$ (n impair), donc $a^{3^j} - 1 = -(2^n + 1)$ et $v_3(2^n + 1) = j + 1$. Comme $n^2 \mid 2^n + 1$: $2j = v_3(n^2) \leq j + 1$, d'où $j = 1$.
- q est impair et $q \neq 3$, donc $q \geq 5$. Comme en 1. : $2^{2n} \equiv 1 \pmod{q}$, et l'ordre k' de 2 modulo q divise $2n = 6m$ et $q - 1$. Les facteurs premiers de m sont $\geq q$: $(q - 1) \wedge m = 1$, donc $k' \wedge m = 1$ et (Gauss) $k' \mid 6$: $q \mid 2^6 - 1 = 63 = 3^2 \times 7$, d'où $q = 7$. Mais $2^3 \equiv 1 \pmod{7}$, donc $2^n \equiv 1$, 2 ou 4 $\pmod{7}$, jamais $-1 \equiv 6$: $7 \nmid 2^n + 1$, contradiction. Donc $m = 1$ et $n = 3$. $n \in \{1, 3\}$ (Olympiade internationale 1990).

29

Corrigés : division euclidienne■ **Corrigé de l'exercice 31**

- a) On a $2026 = 37 \times 54 + 28$ avec $0 \leq 28 < 37$: par **unicité** de la division euclidienne, le quotient est 54 et le reste 28.
b) On change les signes puis on corrige le reste, qui doit être positif :

$$-2026 = 37 \times (-54) - 28 = 37 \times (-55) + (37 - 28) = 37 \times (-55) + 9 \quad (0 \leq 9 < 37).$$

Ensuite $2026 = (-37) \times (-54) + 28$ (quotient -54, reste 28, car $0 \leq 28 < |-37|$), et $-2026 = 37 \times (-55) + 9 = (-37) \times 55 + 9$ (quotient 55, reste 9).

- Le reste de 2026 par b vaut 26 $\iff 2026 = bq + 26$ avec $26 < b \iff b \mid 2000$ et $b > 26$ (alors $q = \frac{2000}{b}$). Or $2000 = 2^4 \times 5^3$ a $5 \times 4 = 20$ diviseurs : 1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 125, 200, 250, 400, 500, 1000, 2000. Réciproquement, chaque diviseur $b > 26$ convient, d'où **11 solutions** :

$$b \in \{40, 50, 80, 100, 125, 200, 250, 400, 500, 1000, 2000\}.$$

- Si $a = nq + r$ et $a' = nq' + r$, alors $a - a' = n(q - q')$: $n \mid a - a'$. Si 2026, 1500 et 1237 ont le même reste, n divise $2026 - 1500 = 526 = 2 \times 263$ et $1500 - 1237 = 263$, donc $n \mid 263$. Or 263 est premier (non divisible par 2, 3, 5, 7, 11, 13, et $17^2 = 289 > 263$), donc $n = 263$. Réciproquement,

$$2026 = 263 \times 7 + 185, \quad 1500 = 263 \times 5 + 185, \quad 1237 = 263 \times 4 + 185 \quad (0 \leq 185 < 263).$$

Une seule solution : $n = 263$, le reste commun étant 185.

■ Corrigé de l'exercice 32

$$1. \overline{2026}^{(7)} = 2 \times 343 + 0 \times 49 + 2 \times 7 + 6 = \boxed{706} \quad \text{et} \quad \overline{101101}^{(2)} = 32 + 8 + 4 + 1 = \boxed{45}.$$

2. a) On regroupe les termes de $N = \sum_{i=0}^{3m+2} x_i 2^i$ par paquets de trois :

$$N = \sum_{j=0}^m (x_{3j} + 2x_{3j+1} + 4x_{3j+2}) 2^{3j} = \sum_{j=0}^m y_j 8^j, \quad 0 \leq y_j \leq 1 + 2 + 4 = 7.$$

Par unicité de l'écriture en base 8, les y_j (débarassés des zéros de tête) sont les chiffres de N en base 8. **Règle** : on découpe l'écriture binaire en paquets de 3 chiffres à partir de la droite ; chaque paquet donne un chiffre en base 8. Comme $16 = 2^4$, on découpe en paquets de 4 chiffres pour la base 16.

b) $101 | 101 | 110 | 101$ donne $N = \overline{5565}^{(8)}$ et $1011 | 0111 | 0101$ donne $N = \overline{B75}^{(16)}$. En base dix : $N = 11 \times 256 + 7 \times 16 + 5 = \boxed{2933}$ (contrôle : $5 \times 512 + 5 \times 64 + 6 \times 8 + 5 = 2933$ ✓).

3. Pour $b \geq 4$, les chiffres 1, 2, 3 sont admis et

$$\overline{121}^{(b)} = b^2 + 2b + 1 = \boxed{(b+1)^2}, \quad \overline{1331}^{(b)} = b^3 + 3b^2 + 3b + 1 = \boxed{(b+1)^3}.$$

Ainsi $1000 = 10^3 = (9+1)^3 = \overline{1331}^{(9)}$ et $343 = 7^3 = (6+1)^3 = \overline{1331}^{(6)}$ (unicité de l'écriture).

4. En base 2 : 2^{2026} s'écrit 1 suivi de 2026 zéros : $\boxed{2027}$ chiffres. Comme $2026 = 3 \times 675 + 1$, $2^{2026} = 2 \times 8^{675} = \overline{20 \dots 0}^{(8)}$ (2 suivi de 675 zéros) : $\boxed{676}$ chiffres en base 8 ; c'est aussi la règle de la question 2 : les 2027 chiffres binaires forment 675 paquets 000 et un paquet de tête 10. Comme $2026 = 4 \times 506 + 2$, $2^{2026} = 4 \times 16^{506} = \overline{40 \dots 0}^{(16)}$ (4 suivi de 506 zéros) : $\boxed{507}$ chiffres en base 16.

■ Corrigé de l'exercice 33

1. On cherche $n \geq 1$ et q tels que $2026 = nq + q$ et $0 \leq q < n$, soit $2026 = q(n+1)$ avec $1 \leq q < n$ ($q \neq 0$ car $2026 \neq 0$).

1013 n'est divisible par aucun des nombres premiers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 (vérification directe) et $31^2 = 961 < 1013 < 32^2$: il est premier. Les diviseurs de $2026 = 2 \times 1013$ sont donc 1, 2, 1013, 2026.

• $n+1 = 2$: $n = 1$ et $q = 1013 \nless 1$; $n+1 = 1013$: $n = 1012$, $q = 2 < 1012$; $n+1 = 2026$: $n = 2025$, $q = 1 < 2025$.

$n \in \{1012, 2025\}$: $2026 = 1012 \times 2 + 2$ et $2026 = 2025 \times 1 + 1$ ✓.

2. On fait apparaître le diviseur : $2^{n+3} + 5 = 8(2^n + 1) - 3 = 7(2^n + 1) + (2^n - 2)$.

• Si $n \geq 1$: $0 \leq 2^n - 2 < 2^n + 1$, donc (unicité) $\boxed{q = 7 \text{ et } r = 2^n - 2}$ (par exemple $n = 3$: $69 = 9 \times 7 + 6$).

• Si $n = 0$: $2^n - 2 = -1 < 0$ ne convient pas ; directement $13 = 2 \times 6 + 1$: $\boxed{q = 6, r = 1}$.

3. a) Écrivons $p = 6k + r$, $0 \leq r \leq 5$. Si $r \in \{0, 2, 4\}$, p est pair et $p > 2$; si $r = 3$, $3 \mid p$ et $p > 3$: dans ces cas p n'est pas premier. Donc $\boxed{r = 1 \text{ ou } r = 5}$.

- b) $p^2 - 1 = (p-1)(p+1)$: si $p = 6k+1$, $3 \mid p-1$; si $p = 6k+5$, $p+1 = 6(k+1)$ et $3 \mid p+1$. De plus p est impair, donc $8 \mid p^2 - 1$ (cours). Comme $3 \wedge 8 = 1$, $24 \mid p^2 - 1$ (corollaire de Gauss). Enfin $p^2 - q^2 = (p^2 - 1) - (q^2 - 1)$ est divisible par 24. (Exemple : $13^2 - 7^2 = 120 = 24 \times 5$.)

■ Corrigé de l'exercice 34

- a) Les multiples de d dans $\{1, \dots, N\}$ sont les kd avec $k \geq 1$ et $kd \leq N$, soit $1 \leq k \leq \frac{N}{d}$. Comme k est entier, $k \leq \frac{N}{d} \iff k \leq E\left(\frac{N}{d}\right)$: il y en a $E\left(\frac{N}{d}\right)$.

b) Si $30 \mid n$, alors $6 \mid n$ et $10 \mid n$. Réciproquement, si $n = 6k$ et $10 \mid 6k$, alors $5 \mid 3k$, donc $5 \mid k$ (Gauss, $5 \wedge 3 = 1$) et $30 \mid n$. Par a), il y a $E\left(\frac{2026}{6}\right) = 337$ multiples de 6, $E\left(\frac{2026}{10}\right) = 202$ multiples de 10, et $E\left(\frac{2026}{30}\right) = 67$ multiples des deux. Il y en a donc $337 + 202 - 67 = 472$.
- Soit $m = E(x)$ et $m = nq + r$ ($0 \leq r \leq n-1$) ; ainsi $E\left(\frac{m}{n}\right) = q$. De $m \leq x < m+1$ on tire $nq \leq nq + r \leq x < nq + r + 1 \leq nq + n$, donc $q \leq \frac{x}{n} < q+1$ et $E\left(\frac{x}{n}\right) = q = E\left(\frac{E(x)}{n}\right)$.

Avec $x = \frac{2026}{5}$ et $n = 7$: $E\left(\frac{2026}{35}\right) = E\left(\frac{E(405,2)}{7}\right) = E\left(\frac{405}{7}\right) = 57$ ($405 = 7 \times 57 + 6$).
- Écrivons $n = mq + r$, $0 \leq r \leq m-1$. Pour $0 \leq k \leq m-1$: $\frac{n+k}{m} = q + \frac{r+k}{m}$ avec $0 \leq r+k \leq 2m-2$, donc $E\left(\frac{n+k}{m}\right) = q+1$ si $k \geq m-r$, et q sinon. Les entiers $k \in \{m-r, \dots, m-1\}$ sont au nombre de r , d'où

$$\sum_{k=0}^{m-1} E\left(\frac{n+k}{m}\right) = mq + r = \boxed{n}. \quad \text{Contrôle : } E\left(\frac{2026}{3}\right) + E\left(\frac{2027}{3}\right) + E\left(\frac{2028}{3}\right) = 675 + 675 + 676 = 2026 \quad \checkmark$$
- On a $a = qb + r$ avec $0 \leq r < q$ (et $q \geq 1$ puisque $q > r \geq 0$) : par unicité, c'est la division euclidienne de a par q , de quotient b et de reste r . Ici $2026 = 37 \times 54 + 28$ avec $28 < 54$, donc $2026 = 54 \times 37 + 28$: quotient 37, reste 28.

■ Corrigé de l'exercice 35

- Existence.** Soit $a = bq_0 + r_0$ la division euclidienne usuelle, $0 \leq r_0 \leq 2m$. Si $r_0 \leq m$, le couple (q_0, r_0) convient. Si $m+1 \leq r_0 \leq 2m$, alors $a = b(q_0 + 1) + (r_0 - b)$ avec $-m \leq r_0 - b \leq -1$.

Unicité. Si $bq + r = bq' + r'$ avec $|r| \leq m$ et $|r'| \leq m$, alors $b|q - q'| = |r' - r| \leq 2m < b$, donc $q = q'$ puis $r = r'$.

Ici $m = 14$ et $25 > 14$: $2026 = 29 \times 70 + (25 - 29) = 29 \times 70 - 4$ (quotient 70, reste -4).
- Initialisation** ($k = 1, M_1 = 1$) : $n \in \{-1, 0, 1\}$ s'écrit $n = \varepsilon_0$ avec $\varepsilon_0 = n$, et c'est la seule écriture.

Hérédité. Supposons la propriété vraie au rang k et soit $|n| \leq M_{k+1}$.

 - Existence** : division centrée $n = 3q + \varepsilon_0$, $\varepsilon_0 \in \{-1, 0, 1\}$. Alors $|q| \leq \frac{M_{k+1}+1}{3} = \frac{3^{k+1}+1}{6} < \frac{3^{k+1}}{2} = M_k + 1$, donc $|q| \leq M_k$. Par hypothèse $q = \sum_{i=0}^{k-1} \varepsilon'_i 3^i$, d'où $n = \varepsilon_0 + \sum_{i=0}^{k-1} \varepsilon'_i 3^{i+1}$: écriture au rang $k+1$.
 - Unicité** : si $n = \sum_{i=0}^k \varepsilon_i 3^i = \sum_{i=0}^k \eta_i 3^i$, alors $n = 3q + \varepsilon_0 = 3q' + \eta_0$ avec $q = \sum_{i=1}^k \varepsilon_i 3^{i-1}$, $q' = \sum_{i=1}^k \eta_i 3^{i-1}$. L'unicité de la division centrée ($m = 1$) donne $\varepsilon_0 = \eta_0$ et $q = q'$; comme $|q| \leq \sum_{i=0}^{k-1} 3^i = M_k$, l'hypothèse de récurrence donne $\varepsilon_i = \eta_i$ pour tout i .

Les 3^k choix des ε_i donnent exactement les $2M_k + 1 = 3^k$ entiers de $[-M_k, M_k]$.
- $2187 - 2026 = 161 = 243 - 81 - 1$, donc $2026 = 3^7 - 3^5 + 3^4 + 1$ ($2187 - 243 + 81 + 1 = 2026 \quad \checkmark$). On le retrouve par divisions centrées successives : $2026 = 3 \times 675 + 1$, $675 = 3 \times 225$, $225 = 3 \times 75$, $75 = 3 \times 25$, $25 = 3 \times 8 + 1$, $8 = 3 \times 3 - 1$, $3 = 3 \times 1$, $1 = 3 \times 0 + 1$.

4. a) Posons l'objet, de masse n , sur le plateau de gauche. Une masse 3^i posée à droite compte $+3^i$, à gauche -3^i , et non utilisée 0 : l'équilibre s'écrit $n = \sum_{i=0}^4 \varepsilon_i 3^i$. Comme $1 \leq n \leq 121 = M_5$, la question 2 fournit une telle écriture. Pour $100 : 100 = 3 \times 33 + 1$, $33 = 3 \times 11$, $11 = 3 \times 4 - 1$, $4 = 3 \times 1 + 1$, $1 = 1$, d'où $100 = 1 - 9 + 27 + 81$: **on place l'objet et la masse de 9 g d'un côté, les masses 1, 27, 81 g de l'autre.**
- b) Chaque masse a trois positions possibles : il y a $3^5 = 243$ dispositions, chacune de valeur $s = (\text{droite}) - (\text{gauche})$. Échanger les plateaux transforme s en $-s$: les dispositions de valeur $s > 0$ sont aussi nombreuses que celles de valeur $s < 0$, et la disposition « aucune masse » vaut 0. Il y a donc au plus $\frac{243-1}{2} = \boxed{121}$ valeurs $s \geq 1$, donc au plus 121 masses différentes : les masses 1, 3, 9, 27, 81 sont optimales.

■ Corrigé de l'exercice 36

1. Comme $0 \leq r_k \leq b-1$, on a $0 \leq 10r_k < 10b$, donc $c_{k+1} = E\left(\frac{10r_k}{b}\right) \in \{0, \dots, 9\}$.
2. Pour $n = 1 : 10a = 10r_0 = bc_1 + r_1 = bN_1 + r_1$. Si $10^n a = bN_n + r_n$, alors

$$10^{n+1}a = 10bN_n + 10r_n = 10bN_n + bc_{n+1} + r_{n+1} = b(10N_n + c_{n+1}) + r_{n+1} = bN_{n+1} + r_{n+1}.$$

En divisant par $b10^n$: $\frac{a}{b} = \frac{N_n}{10^n} + \frac{r_n}{b10^n}$ avec $0 \leq \frac{r_n}{b10^n} < \frac{1}{10^n}$, d'où l'encadrement : $N_n = E\left(10^n \frac{a}{b}\right)$.

3. $10 = 7 \times 1 + 3$, $30 = 7 \times 4 + 2$, $20 = 7 \times 2 + 6$, $60 = 7 \times 8 + 4$, $40 = 7 \times 5 + 5$, $50 = 7 \times 7 + 1$:

$$(r_1, \dots, r_6) = (3, 2, 6, 4, 5, 1), \quad (c_1, \dots, c_6) = (1, 4, 2, 8, 5, 7).$$

Comme $r_6 = r_0$ et que (r_{k+1}, c_{k+1}) ne dépend que de r_k , tout se répète : $\frac{1}{7} = 0,142857\,142857\dots$
Puisque $2026 = 6 \times 337 + 4$, la 2026^e décimale est $c_4 = \boxed{8}$.

4. Les b entiers $r_0, \dots, r_{b-1}$ sont dans $\{1, \dots, b-1\}$, qui n'a que $b-1$ éléments : deux sont égaux, $r_i = r_j$ avec $0 \leq i < j \leq b-1$ (principe des tiroirs). Comme r_{k+1} et c_{k+1} sont le reste et le quotient de $10r_k$ par b , l'égalité $r_{k+T} = r_k$ (vraie pour $k = i$) entraîne $r_{k+1+T} = r_{k+1}$ et $c_{k+1+T} = c_{k+1}$: par récurrence, ces égalités valent pour tout $k \geq i$. **Le développement décimal de $\frac{a}{b}$ est périodique à partir de la $(i+1)^{\text{e}}$ décimale, de période $T \leq b-1$.** (Si un r_k est nul, tous les suivants le sont : le développement est fini.)
5. a) Si $r_n = 0$, alors $b \mid 10^n a$; or $b \wedge 10^n = 1$ (car $b \wedge 10 = 1$), donc $b \mid a$ (Gauss), impossible puisque $0 < a < b$. Si $r_{k+1} = r_{l+1}$, alors $10r_k - bc_{k+1} = 10r_l - bc_{l+1}$, donc $b \mid 10(r_k - r_l)$, puis $b \mid r_k - r_l$ (Gauss) ; comme $|r_k - r_l| < b$, $r_k = r_l$.
- b) En appliquant i fois a) à $r_i = r_j$: $r_{i-1} = r_{j-1}, \dots, r_0 = r_{j-i} = r_T$. La période commence donc dès c_1 .
- c) $\frac{1}{13} : 10 = 13 \times 0 + 10$, $100 = 13 \times 7 + 9$, $90 = 13 \times 6 + 12$, $120 = 13 \times 9 + 3$, $30 = 13 \times 2 + 4$, $40 = 13 \times 3 + 1$, et $r_6 = 1 = r_0$, d'où $\boxed{\frac{1}{13} = 0,076923\,076923\dots}$ ($T = 6$).
- $\frac{1}{12} : 10 = 12 \times 0 + 10$, $100 = 12 \times 8 + 4$, $40 = 12 \times 3 + 4$, ..., d'où $\frac{1}{12} = 0,08333\dots$: la période (3) ne commence qu'à la 3^e décimale, ce qui est permis car $12 \wedge 10 = 2 \neq 1$.

30

Corrigés : congruences et restes■ **Corrigé de l'exercice 37**

1. a) $2^3 = 8 \equiv -1 [9]$, donc $2^6 \equiv 1 [9]$. Comme $2026 = 6 \times 337 + 4$: $2^{2026} = (2^6)^{337} \times 2^4 \equiv 16 \equiv 7 [9]$.
Reste $\boxed{7}$.
- b) $3^3 = 27 \equiv -1 [7]$, donc $3^6 \equiv 1$; $100 = 6 \times 16 + 4$ donne $3^{100} \equiv 3^4 = 81 \equiv 4 [7]$. $4^3 = 64 \equiv 1 [7]$ et $100 = 3 \times 33 + 1$ donnent $4^{100} \equiv 4$. Ainsi $3^{100} + 4^{100} \equiv 8 \equiv 1 [7]$: reste $\boxed{1}$.
- c) $2026 = 17 \times 119 + 3$, donc $2026^{2027} \equiv 3^{2027} [17]$. Or $3^4 = 81 \equiv -4 [17]$, $3^8 \equiv 16 \equiv -1$ et $3^{16} \equiv 1$. Avec $2027 = 16 \times 126 + 11$:

$$3^{2027} \equiv 3^{11} = 3^8 \times 3^3 \equiv -27 \equiv 7 [17]. \quad \text{Reste } \boxed{7}.$$

2. a) $13^2 = 169 \equiv 69$, $13^4 \equiv 69^2 = 4761 \equiv 61 [100]$. Puis $61^2 = 3721 \equiv 21$, $61^4 \equiv 21^2 = 441 \equiv 41$, et $13^{20} \equiv 61^5 \equiv 41 \times 61 = 2501 \equiv 1 [100]$.
- b) $2026 = 20 \times 101 + 6$, donc $13^{2026} \equiv 13^6 = 13^4 \times 13^2 \equiv 61 \times 69 = 4209 \equiv 9 [100]$. Les deux derniers chiffres de 13^{2026} sont $\boxed{0 \text{ puis } 9}$ (il se termine par ... 09).
3. $6^{2n} = 36^n$ et $36 \equiv 3 [11]$, donc $6^{2n} \equiv 3^n$; de plus $3^{n+2} = 9 \times 3^n$. Ainsi

$$6^{2n} + 3^{n+2} + 3^n \equiv 3^n + 9 \times 3^n + 3^n = 11 \times 3^n \equiv 0 [11].$$

■ **Corrigé de l'exercice 38**

1. On calcule x^2 modulo 13 (le tableau est symétrique car $(13 - x)^2 \equiv x^2$) :

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \bmod 13$	0	1	4	9	3	12	10	10	12	3	9	4	1

Un carré a pour reste $\boxed{0, 1, 3, 4, 9, 10 \text{ ou } 12}$ dans la division par 13.

2. a) $5 \times 8 = 40 \equiv 1 [13]$. En multipliant par 8 (et réciproquement par 5) : $5x \equiv 7 \iff x \equiv 56 \equiv 4 [13]$. $\boxed{x \equiv 4 [13]}$ (contrôle : $5 \times 4 = 20 \equiv 7 \checkmark$).
- b) $x^2 + 4x \equiv 6 \iff (x+2)^2 \equiv 10 [13] \iff x+2 \equiv 6 \text{ ou } x+2 \equiv 7 [13]$ (tableau) $\iff \boxed{x \equiv 4 \text{ ou } x \equiv 5 [13]}$.
- c) Comme $8 \times 5 = 40 \equiv 1 [13]$, multiplier par 8 est une équivalence (on revient en multipliant par 5) :

$$2x^2 + 3x + 4 \equiv 0 \iff 16x^2 + 24x + 32 \equiv 0 \iff (4x+3)^2 + 23 \equiv 0 \iff (4x+3)^2 \equiv 3 [13].$$

D'après le tableau, $4x+3 \equiv 4$ ou $4x+3 \equiv 9$, soit $4x \equiv 1$ ou $4x \equiv 6 [13]$; en multipliant par 10 ($4 \times 10 = 40 \equiv 1$) : $\boxed{x \equiv 10 \text{ ou } x \equiv 8 [13]}$ (contrôle : $2 \times 64 + 24 + 4 = 156 = 12 \times 13 \checkmark$).

3. a) Si $x^2 - 13y = 2$, alors $x^2 \equiv 2 [13]$; or 2 n'est pas un reste de carré modulo 13 : **pas de solution**.
- b) $x^2 - 13y = 3 \iff x^2 \equiv 3 [13]$ et $y = \frac{x^2-3}{13} \iff x \equiv 4 \text{ ou } x \equiv 9 [13]$, et $y = \frac{x^2-3}{13}$. Avec $x = 13k+4$: $x^2 - 3 = 169k^2 + 104k + 13$; avec $x = 13k+9$: $x^2 - 3 = 169k^2 + 234k + 78$. D'où

$$S = \{(13k+4, 13k^2+8k+1), (13k+9, 13k^2+18k+6) : k \in \mathbb{Z}\}.$$

■ Corrigé de l'exercice 39

1. a) $27 \times 37 = 999$. Comme $1000 \equiv 1 [999]$, on a $1000^i \equiv 1$, donc $N = \sum t_i 1000^i \equiv \sum t_i [999]$. Une congruence modulo 999 reste vraie modulo tout diviseur de 999, donc $N \equiv t_0 + t_1 + \dots$ modulo 37 et modulo 27. **Critère** : N est divisible par 37 (resp. 27) si et seulement si la somme de ses tranches de trois chiffres l'est (et les restes sont les mêmes).
- b) $123 + 456 + 789 = 1368$, puis $1 + 368 = 369$. Comme $369 = 37 \times 9 + 36 = 27 \times 13 + 18$, le reste de 123 456 789 est $\boxed{36}$ par 37 et $\boxed{18}$ par 27.
2. a) $2N = 20a + 2u \equiv a + 2u [19]$ car $20 \equiv 1$. Si $19 \mid N$, alors $19 \mid 2N$, donc $19 \mid a + 2u$. Réciproquement, si $19 \mid a + 2u$, alors $19 \mid 2N$ et, comme $19 \wedge 2 = 1$, $19 \mid N$ (Gauss).
- b) $87\,723 \rightarrow 8772 + 6 = 8778 \rightarrow 877 + 16 = 893 \rightarrow 89 + 6 = 95 = 5 \times 19$: $\boxed{19 \mid 87\,723}$ (en effet $87\,723 = 19 \times 4617$).
- $2026 \rightarrow 202 + 12 = 214 \rightarrow 21 + 8 = 29$, qui n'est pas multiple de 19 : $\boxed{19 \nmid 2026}$.
3. a) $10 \equiv 1 [9]$, donc $10^i \equiv 1$ et $N = \sum x_i 10^i \equiv \sum x_i = S(N) [9]$.
- b) Si $N + S(N) = 2026$, alors $N \leq 2026$; si $N < 2000$, $S(N) \leq 1 + 9 + 9 + 9 = 28$, et si $2000 \leq N \leq 2026$, $S(N) \leq 2 + 0 + 2 + 9 = 13$. Dans tous les cas $N = 2026 - S(N) \geq 1998$.
- Modulo 9 : $2N \equiv N + S(N) = 2026 \equiv 1 \equiv 10 [9]$; en multipliant par 5 ($2 \times 5 \equiv 1$), $N \equiv 5 [9]$. Les entiers de $[1998, 2025]$ congrus à 5 modulo 9 sont 2003, 2012, 2021 ($1998 = 9 \times 222$), et $2003 + 5 = 2008$, $2012 + 5 = 2017$, $2021 + 5 = 2026$: $\boxed{N = 2021}$ (unique solution).

■ Corrigé de l'exercice 40

1. $2^5 = 32 = 31 + 1 \equiv 1 [31]$. Si $n = 5k + r$ ($0 \leq r \leq 4$), alors $2^n = (2^5)^k 2^r \equiv 2^r [31]$:

$n \equiv \dots [5]$	0	1	2	3	4
reste de 2^n par 31	1	2	4	8	16

2. $2026 = 5 \times 405 + 1$ donne $2^{2026} \equiv 2$; $33 \equiv 2 [31]$ et $2027 = 5 \times 405 + 2$ donnent $33^{2027} \equiv 2^{2027} \equiv 4$. Reste : $\boxed{6}$.
3. a) $A_n = 1 + 2^n + 2^{2n} + 2^{3n} + 2^{4n}$. Si $n \equiv 0 [5]$, chaque terme est congru à 1 : $A_n \equiv 5 [31]$, et $31 \nmid A_n$. Si $n \equiv r [5]$ avec $r \in \{1, 2, 3, 4\}$, les exposants $0, r, 2r, 3r, 4r$ sont, modulo 5, les nombres $0, 1, 2, 3, 4$ dans un certain ordre (par exemple $r = 2$: $0, 2, 4, 6 \equiv 1, 8 \equiv 3$). D'après le tableau, $A_n \equiv 1 + 2 + 4 + 8 + 16 = 31 \equiv 0 [31]$. Donc $\boxed{31 \mid A_n \iff n \not\equiv 0 [5]}$.
- b) Avec $x = 2^n$: $(x-1)A_n = (x-1)(1 + x + x^2 + x^3 + x^4) = x^5 - 1 = 2^{5n} - 1 \equiv 0 [31]$. Si $n \not\equiv 0 [5]$, $2^n \not\equiv 1$, donc $31 \nmid 2^n - 1$; comme 31 est premier et divise le produit, $31 \mid A_n$ (lemme d'Euclide).
4. Soit $n = 5k + r$ ($0 \leq r \leq 4$). Alors $2^n \equiv n [31] \iff n \equiv 2^r [31]$, soit $n = 2^r + 31t$ ($t \in \mathbb{Z}$). Comme $31 \equiv 1 [5]$, $n \equiv 2^r + t [5]$, et la condition $n \equiv r [5]$ s'écrit $t \equiv r - 2^r [5]$:

r	0	1	2	3	4
$t \equiv r - 2^r [5]$	4	4	3	0	3
$n \equiv 2^r + 31t [155]$	125	126	97	8	109

Toutes ces étapes sont des équivalences : $\boxed{2^n \equiv n [31] \iff n \equiv 8, 97, 109, 125 \text{ ou } 126 [155]}$
(contrôle : $2^8 = 256 = 8 \times 31 + 8$ ✓).

■ Corrigé de l'exercice 41

- $365 = 7 \times 52 + 1 \equiv 1 [7]$ et $366 \equiv 2 [7]$: un an plus tard, on a avancé de 365 ou 366 jours, donc d'un ou de deux rangs dans la semaine.
- Entre le 14 octobre 2026 et le 14 octobre 2126, on franchit les 29 février des années bissextiles de 2027 à 2126 : 2028, 2032, ..., 2124, soit $\frac{2124-2028}{4} + 1 = 25$ années, moins 2100 (divisible par 100, pas par 400), donc 24. Le décalage est $100 + 24 = 124 = 7 \times 17 + 5 \equiv 5 [7]$ (on a bien $100 \times 365 + 24 = 36\,524 \equiv 5$). Mercredi + 5 : le 14 octobre 2126 sera un lundi.
- Parmi 400 entiers consécutifs, il y a exactement 100 multiples de 4, 4 multiples de 100 et 1 multiple de 400 : 400 années consécutives comptent $100 - 4 + 1 = 97$ années bissextiles, donc $400 \times 365 + 97 = \text{146 097} = 7 \times 20\,871$ jours. Une date et la même date 400 ans plus tard tombent donc le même jour de la semaine ; comme la règle des années bissextiles ne dépend que du millésime modulo 400, tout le calendrier se répète.
- a) Les mois comptent $31 \equiv 3$, $30 \equiv 2$, $28 \equiv 0$ ou $29 \equiv 1$ jours modulo 7. En cumulant (de janvier à novembre) :

mois m	1	2	3	4	5	6	7	8	9	10	11	12
d_m (non bissextile)	0	31	59	90	120	151	181	212	243	273	304	334
reste modulo 7	0	3	3	6	1	4	6	2	5	0	3	5
reste (bissextile)	0	3	4	0	2	5	0	3	6	1	4	6

- b) Si le 13 janvier a le rang j , le 13 du mois m a le rang $j + d_m$ modulo 7. Dans les deux cas, les restes des d_m prennent **les sept valeurs** 0, 1, ..., 6 : chaque jour de la semaine, en particulier le vendredi, est celui d'au moins un 13 du mois. Une même valeur apparaît au plus trois fois (3 pour février, mars, novembre ; 0 pour janvier, avril, juillet en année bissextile) : **au plus trois vendredis 13**.

2026 n'est pas bissextile et $d_2 \equiv d_3 \equiv d_{11} \equiv 3$: les vendredis 13 de 2026 sont **le 13 février, le 13 mars et le 13 novembre**.

■ Corrigé de l'exercice 42

- D'après le cours (Fermat), $30 \mid n^5 - n$, donc $10 \mid n^5 - n \equiv n [10]$. Pour $k \geq 1$: $n^{k+4} - n^k = n^{k-1}(n^5 - n) \equiv 0 [10]$. Par récurrence sur j : $n^{k+4(j+1)} = n^{(k+4j)+4} \equiv n^{k+4j} \equiv n^k [10]$, car $k + 4j \geq 1$.
- $n + 20 \equiv n [10]$, donc $(n + 20)^{n+20} \equiv n^{n+20} [10]$ (compatibilité avec les puissances) ; puis $n^{n+20} = n^{n+4 \times 5} \equiv n^n [10]$ (question 1 avec $k = n \geq 1, j = 5$). Les chiffres des unités étant les restes modulo 10 : $u_{n+20} = u_n$.
- D'après 1, u_n est le chiffre des unités de c^e , où c est le chiffre des unités de n et $e \in \{1, 2, 3, 4\}$, $e \equiv n [4]$. Par exemple $u_7 : 7^3 = 343$, $u_{12} : 2^4 = 16$, $u_{18} : 8^2 = 64$, $u_{19} : 9^3 = 729$.

n	1	2	3	4	5	6	7	8	9	10
u_n	1	4	7	6	5	6	3	6	9	0
n	11	12	13	14	15	16	17	18	19	20
u_n	1	6	3	6	5	6	7	4	9	0

$u_1 + \dots + u_{10} = 47$ et $u_{11} + \dots + u_{20} = 47$: la somme vaut 94. Comme $u_{12} = 6 \neq u_2 = 4$, 10 **n'est pas une période**.

4. $n^n \equiv u_n [10]$, donc $S \equiv \sum_{n=1}^{2026} u_n [10]$. Comme $2026 = 20 \times 101 + 6$ et que (u_n) est 20-périodique :

$$\sum_{n=1}^{2026} u_n = 101 \times 94 + (u_1 + \dots + u_6) = 9494 + 29 = 9523.$$

Le chiffre des unités de S est $\boxed{3}$.

31

Corrigés : PGCD et Bézout

■ Corrigé de l'exercice 43

1. a) On applique $a \wedge b = b \wedge r$ à chaque division :

$$\begin{aligned} 1512 &= 1092 \times 1 + 420, & 1092 &= 420 \times 2 + 252, & 420 &= 252 \times 1 + 168, \\ 252 &= 168 \times 1 + 84, & 168 &= 84 \times 2 + 0. \end{aligned}$$

Le dernier reste non nul est le PGCD : $\boxed{1512 \wedge 1092 = 84}$.

b) Les diviseurs communs sont les diviseurs de $84 = 2^2 \times 3 \times 7$, au nombre de $3 \times 2 \times 2 = 12$: 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84. Comme $1092 = 84 \times 13$ et $1512 = 84 \times 18$, avec $13 \wedge 18 = 1$

(sinon 84 ne serait pas le PGCD) : $\boxed{\frac{1092}{1512} = \frac{13}{18}}$.

c) $1512 = 2^3 \times 3^3 \times 7$ et $1092 = 2^2 \times 3 \times 7 \times 13$: le PGCD est $2^2 \times 3 \times 7 = 84$ ✓.

2. En centimètres, la salle mesure 1512×1092 . Le côté c d'un carreau doit diviser 1512 et 1092, donc diviser 84 : le plus grand est $\boxed{c = 84 \text{ cm}}$. Il faut alors $18 \times 13 = \boxed{234}$ carreaux.

3. Si $d \mid a$ et $d \mid b$, alors $d \mid a - b$; si $d \mid a - b$ et $d \mid b$, alors $d \mid (a - b) + b = a$. Les couples (a, b) et $(a - b, b)$ ont les mêmes diviseurs communs, donc le même PGCD.

$$(1512, 1092) \rightarrow (420, 1092) \rightarrow (420, 672) \rightarrow (420, 252) \rightarrow (168, 252) \rightarrow (168, 84) \rightarrow (84, 84),$$

soit $\boxed{6 \text{ soustractions}}$. Chaque division de quotient q regroupe q soustractions, sauf la dernière où l'on s'arrête à l'égalité : $1 + 2 + 1 + 1 + (2 - 1) = 6$.

■ Corrigé de l'exercice 44

On utilise $x \wedge y = (x - ky) \wedge y$ pour tout $k \in \mathbb{Z}$.

1. Posons $A = n^4 + 3n^2 + 1$ et $B = n^3 + 2n$. Alors $A - nB = n^2 + 1$, $B - n(n^2 + 1) = n$ et $(n^2 + 1) - n \times n = 1$. Donc

$$A \wedge B = B \wedge (n^2 + 1) = (n^2 + 1) \wedge n = n \wedge 1 = 1 : \text{ la fraction est irréductible.}$$

2. $n^2 + 1 - (n - 1)(n + 1) = 2$, donc $(n + 1) \wedge (n^2 + 1) = (n + 1) \wedge 2 \in \{1, 2\}$. Il vaut $\boxed{2 \text{ si } n \text{ est impair}}$ et $\boxed{1 \text{ si } n \text{ est pair}}$.

3. Soit d ce PGCD. Comme $(n + 1)! + 1 - (n + 1)(n! + 1) = -n$, on a $d \mid n$. Or $n \geq 1$ divise $n!$, donc $d \mid n!$; avec $d \mid n! + 1$, on obtient $d \mid 1$: $\boxed{d = 1}$. Pour $n = 0$: $0! + 1 = 1! + 1 = 2$, et le PGCD vaut 2 : **le résultat est faux** (l'argument utilisait $n \mid n!$, faux pour $n = 0$).

■ Corrigé de l'exercice 45

- Soit $d = a \wedge b$. Au départ, les deux récipients contiennent 0. Supposons qu'avant une opération, les contenus x et y soient multiples de d . Remplir donne a ou b , vider donne 0 ; transvaser x dans l'autre récipient donne soit $(0, x + y)$, soit $(x - (b - y), b)$ (ou les analogues avec a) : tous ces nombres sont des combinaisons de x, y, a, b à coefficients entiers, donc des multiples de d . Avec 9 et 6 litres, $d = 3$: on n'obtient que des multiples de 3 litres, **jamais 1 litre**.
- $9 = 7 \times 1 + 2$ et $7 = 2 \times 3 + 1$, d'où $1 = 7 - 3 \times 2 = 7 - 3(9 - 7) = \boxed{7 \times 4 - 9 \times 3}$: $(u, v) = (4, 3)$.
Interprétation : en versant 4 fois le contenu de B (28 litres) dans A , et en vidant 3 fois A plein (27 litres), il reste exactement 1 litre.
- a) On verse 7 litres dans A qui contient $r_{k-1} \leq 8$: comme $r_{k-1} + 7 \leq 15 < 18$, on vide A au plus une fois. Si $r_{k-1} + 7 \leq 8$, $r_k = r_{k-1} + 7$; sinon $r_k = r_{k-1} + 7 - 9$ (y compris le cas $r_{k-1} + 7 = 9$, où A plein est vidé). Ainsi $r_k \equiv r_{k-1} + 7 [9]$ et $0 \leq r_k \leq 8$. Par récurrence, $r_k \equiv 7k [9]$ avec $0 \leq r_k < 9$: **r_k est le reste de $7k$ par 9**.
b) Si $1 \leq k \leq 8$, $9 \nmid 7k$ (Gauss, $9 \wedge 7 = 1$), donc $r_k \neq 0$. Si $r_k = r_l$, alors $9 \mid 7(k - l)$, donc $9 \mid k - l$ et $k = l$ pour $1 \leq k, l \leq 8$. Les 8 restes sont distincts dans $\{1, \dots, 8\}$: ce sont tous ces entiers ($r_1, \dots, r_8 = 7, 5, 3, 1, 8, 6, 4, 2$). **On peut obtenir dans A toute quantité entière de 1 à 8 litres**.
c) $r_k = 4 \iff 7k \equiv 4 [9] \iff k \equiv 4 \times 4 = 16 \equiv 7 [9]$ (car $7 \times 4 = 28 \equiv 1$) : il faut $\boxed{7}$ remplissages de B . En échangeant les rôles, la quantité dans B est le reste de $9k \equiv 2k$ par 7, et $2k \equiv 4 [7] \iff k \equiv 2 [7]$: $\boxed{2}$ remplissages de A suffisent ($18 = 7 \times 2 + 4$).

■ Corrigé de l'exercice 46

- Écrivons $a = da'$, $b = db'$ avec $a' \wedge b' = 1$ (cours). Alors $a'^2 \wedge b'^2 = 1$ (cours : $a^m \wedge b^n = 1$), et

$$a^2 \wedge b^2 = (d^2 a'^2) \wedge (d^2 b'^2) = d^2 (a'^2 \wedge b'^2) = \boxed{d^2}.$$
- a) Soit $g = \delta \wedge a$. Alors $g \mid a$ et $g \mid \delta \mid a + b$, donc $g \mid b$; ainsi $g \mid a \wedge b = 1$. De même $\delta \wedge b = 1$, d'où $\delta \wedge ab = 1$ (cours).
b) $\delta \mid a + b$, donc $\delta \mid (a + b)^2$; et $\delta \mid a^2 - ab + b^2 = (a + b)^2 - 3ab$. Donc $\delta \mid 3ab$ et, comme $\delta \wedge ab = 1$, $\delta \mid 3$ (Gauss). Si $3 \mid a + b$, alors $3 \mid (a + b)^2 - 3ab$, donc $3 \mid \delta$ et $\boxed{\delta = 3}$; sinon $3 \nmid \delta$ (car $\delta \mid a + b$) et $\boxed{\delta = 1}$.
c) $(2026, 1)$: $a + b = 2027$ et $2 + 0 + 2 + 7 = 11$, donc $3 \nmid 2027$: $\delta = 1$, c'est-à-dire $2027 \wedge (2026^2 - 2026 + 1) = 1$. $(5, 4)$: $a + b = 9$ et $a^2 - ab + b^2 = 21$: $\delta = 9 \wedge 21 = 3$ ($5^3 + 4^3 = 189 = 9 \times 21$).
- Soit d ce PGCD. Comme $(n + 1)^2 + 2 - (n^2 + 2) = 2n + 1$, on a $d = (n^2 + 2) \wedge (2n + 1)$, et

$$d \mid 4(n^2 + 2) - (2n - 1)(2n + 1) = 8 + 1 = 9 \quad \text{donc} \quad d \in \{1, 3, 9\}.$$

 $3 \mid 2n + 1 \iff 2n \equiv 2 [3] \iff n \equiv 1 [3]$, et alors $n^2 + 2 \equiv 3 \equiv 0 [3]$: $3 \mid d \iff n \equiv 1 [3]$.
 $9 \mid 2n + 1 \iff 2n \equiv 8 [9] \iff n \equiv 4 [9]$ (on multiplie par 5), et alors $n^2 + 2 \equiv 18 \equiv 0 [9]$: $9 \mid d \iff n \equiv 4 [9]$.
 Conclusion : $\boxed{d = 9 \iff n \equiv 4 [9]}$, $\boxed{d = 3 \iff n \equiv 1 \text{ ou } 7 [9]}$, $d = 1$ sinon (contrôles : $n = 4$: $18 \wedge 27 = 9$; $n = 1$: $3 \wedge 6 = 3$).
- Soit d ce PGCD : $d \mid (2^{n+1} + 3^{n+1}) - 2(2^n + 3^n) = 3^n$ et $d \mid 3(2^n + 3^n) - (2^{n+1} + 3^{n+1}) = 2^n$. Comme $2 \wedge 3 = 1$, $2^n \wedge 3^n = 1$ (cours), donc $\boxed{d = 1}$.

■ Corrigé de l'exercice 47

1. De $c \times b + d \times (-a) = 1$ et $a \times (-d) + b \times c = 1$, le théorème de Bézout donne $c \wedge d = 1$ et $a \wedge b = 1$.
Pour la médiane :

$$b(a+c) - a(b+d) = bc - ad = 1 \quad \text{et} \quad (b+d)c - (a+c)d = bc - ad = 1.$$

Donc $\frac{a}{b}$ et $\frac{a+c}{b+d}$ sont voisines, ainsi que $\frac{a+c}{b+d}$ et $\frac{c}{d}$ (la médiane est donc irréductible) ; de plus $\frac{a+c}{b+d} - \frac{a}{b} = \frac{1}{b(b+d)} > 0$ et $\frac{c}{d} - \frac{a+c}{b+d} = \frac{1}{d(b+d)} > 0$.

2. a) $\frac{p}{q} - \frac{a}{b} = \frac{pb-aq}{bq} > 0$, donc l'entier $pb - aq$ est ≥ 1 ; de même $\frac{c}{d} - \frac{p}{q} = \frac{cq-pd}{dq} > 0$ donne $cq - pd \geq 1$.
Puis

$$d(pb - aq) + b(cq - pd) = bdp - adq + bcq - bdp = q(bc - ad) = q.$$

- b) Avec $X = pb - aq \geq 1$ et $Y = cq - pd \geq 1$: $q = dX + bY \geq d + b$, avec égalité si et seulement si $X = Y = 1$. Si $q = b + d$ et $X = 1$: $pb = 1 + a(b+d) = ab + bc = (a+c)b$ (car $1 + ad = bc$), donc $p = a + c$. Réciproquement, la médiane a pour dénominateur $b + d$.

3. a) $18 \times 8 - 13 \times 11 = 144 - 143 = 1$: elles sont voisines. Toute fraction strictement comprise entre elles a un dénominateur $\geq 18 + 11 = 29$, avec égalité pour la seule médiane : la réponse est

$$\boxed{\frac{21}{29}}.$$

- b) Comme $a \wedge b = 1$, Bézout fournit $(c_0, d_0) \in \mathbb{Z}^2$ tel que $bc_0 - ad_0 = 1$. Soit $d_0 = bk + d$ la division euclidienne de d_0 par b ($0 \leq d \leq b-1$) et $c = c_0 - ak$: alors $bc - ad = bc_0 - ad_0 = 1$. On a $d \neq 0$ (sinon $bc = 1$ et $b = 1$), donc $1 \leq d \leq b-1$, et $\frac{c}{d} - \frac{a}{b} = \frac{1}{bd} > 0$.

Pour $\frac{13}{18}$: $18 = 13 + 5$, $13 = 2 \times 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$, d'où $1 = 7 \times 13 - 5 \times 18$, soit $18 \times (-5) - 13 \times (-7) = 1$. Avec $d_0 = -7 = 18 \times (-1) + 11$: $d = 11$ et $c = -5 + 13 = 8$, d'où la voisine

$$\boxed{\frac{8}{11}}.$$

4. Produits en croix : $500 < 504$, $792 < 800$, $800 < 803$, $292 < 300$, d'où la chaîne d'inégalités ; et $7 \times 8 - 5 \times 11 = 1$, $11 \times 3 - 8 \times 4 = 1$. Si le joueur a réussi p tirs sur q , alors $\frac{5}{7} < \frac{p}{q} < \frac{3}{4}$. Si $\frac{p}{q} = \frac{8}{11}$, q est multiple de 11 ($\frac{8}{11}$ est irréductible) ; si $\frac{p}{q} < \frac{8}{11}$, $q \geq 7 + 11 = 18$; si $\frac{p}{q} > \frac{8}{11}$, $q \geq 11 + 4 = 15$. Comme 8 tirs réussis sur 11 donnent bien un taux de 72,7 %, le nombre minimal de tirs est $\boxed{11}$.

■ Corrigé de l'exercice 48

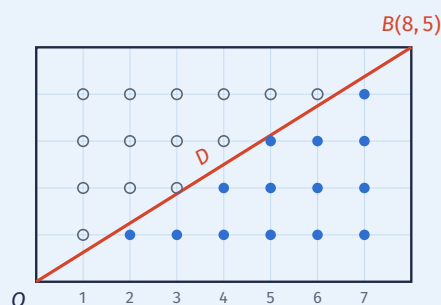
1. a) Si $r_k = 0$, alors $b \mid ka$, donc $b \mid k$ (Gauss, $a \wedge b = 1$) : impossible car $1 \leq k \leq b-1$. Si $r_k = r_l$ avec $k > l$, alors $b \mid (k-l)a$, donc $b \mid k-l$: impossible car $1 \leq k-l \leq b-2$. Les $b-1$ restes sont distincts et dans $\{1, \dots, b-1\}$, qui a $b-1$ éléments : ce sont tous ces entiers.

b) En sommant pour $k = 1, \dots, b-1$: $a \frac{b(b-1)}{2} = bS(a, b) + (1+2+\dots+(b-1)) = bS(a, b) + \frac{b(b-1)}{2}$,

d'où $S(a, b) = \frac{(a-1)(b-1)}{2}$.

2. a) Les points entiers intérieurs d'abscisse k ($1 \leq k \leq b-1$) sous D ou sur D sont les (k, j) avec $1 \leq j \leq \frac{ka}{b}$, soit $1 \leq j \leq E\left(\frac{ka}{b}\right)$ (et $E\left(\frac{ka}{b}\right) \leq a-1$ car $\frac{ka}{b} < a$) : il y en a $E\left(\frac{ka}{b}\right)$. On somme sur k .

- b) Si (k, j) intérieur est sur D , alors $jb = ka$, donc $b \mid k$ (Gauss) : impossible. La symétrie de centre $\Omega\left(\frac{b}{2}, \frac{a}{2}\right)$, $(x, y) \mapsto (b-x, a-y)$, conserve les points entiers intérieurs et D , et échange les deux côtés de D . Les $(a-1)(b-1)$ points intérieurs se partagent donc également : $S(a, b) = \frac{(a-1)(b-1)}{2}$. Pour $a = 5$, $b = 8$ (figure) : $0 + 1 + 1 + 2 + 3 + 3 + 4 = 14 = \frac{4 \times 7}{2}$ points pleins sous la diagonale.



14 points pleins sous D , 14 vides au-dessus

3. Écrivons $a = da'$, $b = db'$ avec $a' \wedge b' = 1$. Un point entier (k, j) intérieur est sur $D \iff jb = ka \iff jb' = ka' \iff b' \mid k$ (Gauss), avec alors $j = \frac{ka'}{b'}$: ce sont les points (mb', ma') , $1 \leq m \leq d-1$, **au nombre de** $d-1$. Par la même symétrie, les $(a-1)(b-1) - (d-1)$ autres points intérieurs se répartissent également de part et d'autre de D , et $S(a, b)$ compte aussi les $d-1$ points de D :

$$S(a, b) = \frac{(a-1)(b-1) - (d-1)}{2} + (d-1) = \frac{(a-1)(b-1) + d-1}{2}.$$

4. $a = 8$, $b = 12$, $d = 4$: $\sum_{k=1}^{11} E\left(\frac{8k}{12}\right) = \frac{7 \times 11 + 3}{2} = \boxed{40}$. Puis $2026 = 2 \times 1013$ (1013 premier, exercice 33) et $1155 = 3 \times 5 \times 7 \times 11$, donc $2026 \wedge 1155 = 1$ et

$$\sum_{k=1}^{2025} E\left(\frac{1155k}{2026}\right) = \frac{1154 \times 2025}{2} = 577 \times 2025 = \boxed{1\,168\,425}.$$

32

Corrigés : Gauss et nombres premiers■ **Corrigé de l'exercice 49**

1. a) $25^2 = 625 < 643 < 676 = 26^2$: il suffit de tester les nombres premiers $p \leq 25$. 643 est impair, la somme de ses chiffres (13) n'est pas divisible par 3, il ne se termine ni par 0 ni par 5, et

$$643 = 7 \times 91 + 6 = 11 \times 58 + 5 = 13 \times 49 + 6 = 17 \times 37 + 14 = 19 \times 33 + 16 = 23 \times 27 + 22.$$

Aucun nombre premier $p \leq 25$ ne divise 643 : 643 est **premier**.

- b) $25^2 < 667 < 26^2$; on teste : $667 = 23 \times 29$, donc 667 **n'est pas premier**.

2. Si $p \equiv 1 [3]$, alors $p + 14 \equiv 15 \equiv 0 [3]$ et $p + 14 > 3$: $p + 14$ n'est pas premier. Si $p \equiv 2 [3]$, alors $p + 10 \equiv 12 \equiv 0 [3]$ et $p + 10 > 3$: $p + 10$ n'est pas premier. Donc $p \equiv 0 [3]$: le nombre premier p est divisible par 3, d'où $p = 3$. Réciproquement 3, 13 et 17 sont premiers ✓.

3. a) $f(0) = 41, f(1) = 43, f(2) = 47, f(3) = 53, f(4) = 61, f(5) = 71$: ils sont premiers (aucun n'est divisible par 2, 3, 5 ou 7, et $71 < 11^2$).

- b) $n(n+1)$ est le produit de deux entiers consécutifs, donc il est pair et $f(n)$ est **impair**. Comme $41 \equiv 2 [3], 41 \equiv 1 [5]$ et $41 \equiv 6 [7]$:

$n [3]$	0	1	2
$n(n+1)$	0	2	0
$f(n)$	2	1	2

$n [5]$	0	1	2	3	4
$n(n+1)$	0	2	1	2	0
$f(n)$	1	3	2	3	1

$n [7]$	0	1	2	3	4	5	6
$n(n+1)$	0	2	6	5	6	2	0
$f(n)$	6	1	5	4	5	1	6

Le reste 0 n'apparaît jamais : $f(n)$ n'est divisible ni par 3, ni par 5, ni par 7.

- c) $f(n) = n(n+1) + 41 \equiv n(n+1) [41]$. Comme 41 est premier, le lemme d'Euclide donne : $41 \mid n(n+1) \iff 41 \mid n$ ou $41 \mid n+1$, soit $n \equiv 0$ ou $n \equiv 40 [41]$.

- d) $f(40) = 1600 + 40 + 41 = 1681 = 41^2$ et $f(41) = 41^2 + 41 + 41 = 41 \times 43 = 1763$. Ces deux nombres ne sont pas premiers : $f(n)$ **n'est pas toujours premier** (alors qu'il l'est pour $0 \leq n \leq 39$).

■ **Corrigé de l'exercice 50**

1. $72 = 2^3 \times 3^2$ et $54 = 2 \times 3^3$. Donc $72 \wedge 54 = 2 \times 3^2 = 18$ et $\text{PPCM}(72, 54) = 2^3 \times 3^3 = 216$ (contrôle : $18 \times 216 = 3888 = 72 \times 54$ ✓).

2. En divisant par 18 : $72x = 54y \iff 4x = 3y$. Alors $3 \mid 4x$ et $3 \wedge 4 = 1$, donc $3 \mid x$ (Gauss) : $x = 3k$, puis $4 \times 3k = 3y$, soit $y = 4k$. Réciproquement ces couples conviennent : $(x, y) = (3k, 4k), k \in \mathbb{N}$.

3. Les deux repères sont de nouveau en contact lorsque chaque roue a fait un nombre entier de tours. Le premier instant correspond à $k = 1$: A a fait **3 tours**, B **4 tours**, et 216 dents sont passées : c'est le PPCM de 72 et 54.

4. La dent marquée de A revient au contact pour la j -ième fois ($j \geq 1$) après le passage de $72j$ dents ; la dent de B alors au contact porte le numéro r_j , reste de $72j$ modulo 54. Or $72j = 54j + 18j$, donc $r_j \equiv 18j [54]$: selon que $j \equiv 0, 1$ ou $2 [3]$, on obtient $r_j = 0, 18$ ou 36 . La dent marquée de A ne rencontre que les dents **0, 18 et 36** de B, les multiples de $72 \wedge 54 = 18$.

5. À chaque point de contact passe le même nombre N de dents. Les trois roues sont dans leur position initiale si et seulement si N est multiple de 72, de 54 et de $90 = 2 \times 3^2 \times 5$, c'est-à-dire de leur PPCM $2^3 \times 3^3 \times 5 = 1080$. La première fois, $N = 1080$:

A fait 15 tours, B en fait 20 et C en fait 12.

■ Corrigé de l'exercice 51

1. En multipliant $P\left(\frac{p}{q}\right) = 0$ par q^n : $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$. Donc

$$a_0 q^n = -p(a_n p^{n-1} + \dots + a_1 q^{n-1}) \quad \text{et} \quad a_n p^n = -q(a_{n-1} p^{n-1} + \dots + a_0 q^{n-1}) :$$

$p \mid a_0 q^n$ et $q \mid a_n p^n$. Comme $p \wedge q = 1$, on a $p \mid a_0$ et $q \mid a_n$.
donne $p \mid a_0$ et $q \mid a_n$.

2. a) $p \mid 2$ et $q \mid 6$ avec $q > 0$: $p \in \{\pm 1, \pm 2\}$ et $q \in \{1, 2, 3, 6\}$. Les candidats sont

$$\pm 1, \pm 2, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{6}.$$

b) $P(2) = 48 - 44 - 6 + 2 = 0$, d'où $P(x) = (x - 2)(6x^2 + x - 1)$. Le trinôme a pour discriminant 25 et pour racines $\frac{-1 \pm 5}{12}$, soit $\frac{1}{3}$ et $-\frac{1}{2}$. Ainsi

$$P(x) = (x - 2)(2x + 1)(3x - 1) \quad \text{racines rationnelles : } 2, -\frac{1}{2}, \frac{1}{3}.$$

3. $\alpha^2 = 8 + 2\sqrt{15}$, donc $(\alpha^2 - 8)^2 = 60$, soit $\alpha^4 - 16\alpha^2 + 4 = 0$. Si α était rationnel, ce serait une racine de $Q(x) = x^4 - 16x^2 + 4$; d'après 1 ($a_n = 1$), on aurait $q = 1$ et $p \mid 4$, donc $\alpha \in \{\pm 1, \pm 2, \pm 4\}$. Or $Q(\pm 1) = -11$, $Q(\pm 2) = -44$ et $Q(\pm 4) = 4$: aucun ne convient. $\alpha = \sqrt{3} + \sqrt{5}$ est irrationnel.

4. Si $\sqrt[3]{m} = \frac{p}{q}$ (forme irréductible), c'est une racine de $x^3 - m$, de coefficient dominant 1 : donc $q = 1$ et $\sqrt[3]{m} = p$ est un entier, d'où $m = p^3$. Comme $2^3 = 8 < 12 < 27 = 3^3$, 12 n'est pas un cube : $\sqrt[3]{12}$ est irrationnel.

■ Corrigé de l'exercice 52

1. a) $5292 = 4 \times 1323 = 4 \times 27 \times 49$, donc $N = 2^2 \times 3^3 \times 7^2$ et $d(N) = (2+1)(3+1)(2+1) = 36$.
b) Les diviseurs positifs de N sont les $2^a 3^b 7^c$ avec $0 \leq a \leq 2$, $0 \leq b \leq 3$, $0 \leq c \leq 2$. Pairs : $a \in \{1, 2\}$, soit $2 \times 4 \times 3 = 24$. Carrés : a, b, c pairs, soit $a \in \{0, 2\}$, $b \in \{0, 2\}$, $c \in \{0, 2\}$: 8.
c) kN est un carré si et seulement si tous ses exposants sont pairs : k doit contenir une puissance impaire de 3, et $k = 3$ convient : $3N = 2^2 \times 3^4 \times 7^2 = 126^2$. Pour un cube, les exposants doivent être multiples de 3 : le plus petit k est $2 \times 7 = 14$, et $14N = 2^3 \times 3^3 \times 7^3 = 42^3 = 74088$.
2. a) Si $\delta \mid n$, alors $n = \delta \times \frac{n}{\delta}$, donc $\frac{n}{\delta}$ est un diviseur positif de n ; l'application $\delta \mapsto \frac{n}{\delta}$ est sa propre réciproque, c'est une bijection. Le produit des diviseurs est donc aussi le produit des $\frac{n}{\delta}$:

$$\Pi(n)^2 = \prod_{\delta \mid n} \delta \times \prod_{\delta \mid n} \frac{n}{\delta} = \prod_{\delta \mid n} n = n^{d(n)}, \quad \text{soit} \quad \Pi(n) = n^{d(n)/2}.$$

$$\text{b) } \Pi(N) = N^{36/2} = N^{18} = 2^{36} \times 3^{54} \times 7^{36}.$$

3. a) Pour $n \geq 2$, $n^{d(n)/2} = n^3 \iff d(n) = 6$. Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, alors $d(n) = (\alpha_1 + 1) \cdots (\alpha_k + 1)$ est un produit de facteurs ≥ 2 ; or 6 s'écrit 6 ou 2×3 : soit $k = 1$ et $\alpha_1 = 5$, soit $k = 2$ et les exposants sont 1 et 2 : $n = p^5$ ou $n = p^2 q$.
- b) $p^5 \leq 50$: 32. $p^2 q \leq 50$: $p = 2$ et $q \in \{3, 5, 7, 11\}$, $p = 3$ et $q \in \{2, 5\}$, $p = 5$ et $q = 2$. D'où

$$n \in \{12, 18, 20, 28, 32, 44, 45, 50\}.$$

4. Soit A l'ensemble des diviseurs $\delta < \sqrt{n}$ et B celui des diviseurs $\delta > \sqrt{n}$. D'après 2.a), $\delta \mapsto \frac{n}{\delta}$ échange A et B , donc $\text{card } B = \text{card } A$. Or $A \subset \{k \in \mathbb{N}^* : k < \sqrt{n}\}$, qui a strictement moins de $\sqrt{n}$ éléments.
- Si n n'est pas un carré : $d(n) = 2 \text{ card } A < 2\sqrt{n}$.
 - Si $n = m^2$: $\text{card } A \leq m - 1$ et $d(n) = 2 \text{ card } A + 1 \leq 2m - 1 < 2\sqrt{n}$.
- Ainsi $d(n) < 2\sqrt{n}$ (par exemple $d(12) = 6 < 2\sqrt{12} \approx 6,93$).

■ Corrigé de l'exercice 53

- Si $a \equiv b \equiv 1 [4]$, alors $ab \equiv 1 \times 1 = 1 [4]$; par récurrence sur le nombre de facteurs, tout produit fini d'entiers congrus à 1 modulo 4 est congru à 1 modulo 4.
- n est impair, donc ses diviseurs premiers sont impairs, congrus à 1 ou 3 modulo 4. S'ils étaient tous congrus à 1, leur produit (avec multiplicité), égal à n , serait congru à 1 modulo 4 d'après 1 : contradiction. Donc n a un diviseur premier $p \equiv 3 [4]$.
- 3 est l'un des p_i , donc $N \geq 4 \times 3 - 1 = 11$, et $N \equiv -1 \equiv 3 [4]$. D'après 2, N a un diviseur premier $p \equiv 3 [4]$, c'est-à-dire $p = p_i$ pour un certain i . Alors $p_i \mid 4p_1 \cdots p_k$ et $p_i \mid N$, donc $p_i \mid 4p_1 \cdots p_k - N = 1$: absurde. **Il existe une infinité de nombres premiers congrus à 3 modulo 4.**
- a) Si $p \equiv 0, 2$ ou $4 [6]$, p est pair et $p > 2$; si $p \equiv 3 [6]$, $3 \mid p$ et $p > 3$. Ces cas sont exclus : $p \equiv 1$ ou $5 [6]$.
b) Supposons qu'il n'y en ait qu'un nombre fini $q_1 = 5, q_2 = 11, \dots, q_k$, et posons $N = 6q_1 \cdots q_k - 1 \geq 29$. Comme $N \equiv 5 [6]$, N n'est divisible ni par 2 ni par 3 : ses diviseurs premiers sont ≥ 5 , donc congrus à 1 ou 5 modulo 6. Un produit d'entiers congrus à 1 modulo 6 est congru à 1 modulo 6 : N a donc un diviseur premier congru à 5 modulo 6, c'est un q_i , et $q_i \mid 6q_1 \cdots q_k - N = 1$: absurde. **Il y a une infinité de premiers congrus à 5 modulo 6.**
- Un entier $N \equiv 1 [4]$ peut n'avoir que des diviseurs premiers congrus à 3 modulo 4 (en nombre pair), par exemple $21 = 3 \times 7$. L'argument de la question 2 ne fournit donc aucun diviseur premier congru à 1 modulo 4. (On y parvient avec $N = 4(p_1 \cdots p_k)^2 + 1$: voir l'exercice 20.)

■ Corrigé de l'exercice 54

- $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \times 6$ et $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \times 28$ ✓. Les diviseurs positifs de p^a sont les p^j , $0 \leq j \leq a$ (unicité de la décomposition), donc $\sigma(p^a) = 1 + p + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$ (somme géométrique).
- a) $d_1 = d \wedge a$ divise d et a : on écrit $d = d_1 d_2$ et $a = d_1 a'$ avec $d_2 \wedge a' = 1$ (cours). Comme $d \mid ab$: $d_1 d_2 \mid d_1 a' b$, donc $d_2 \mid a' b$, et le théorème de Gauss donne $d_2 \mid b$.

b) $d_1 \mid d'_1 d'_2$, et $d_1 \wedge d'_2 = 1$ (un diviseur commun divise a et b). Par Gauss, $d_1 \mid d'_1$; de même $d'_1 \mid d_1$, donc $d_1 = d'_1$ (positifs) puis $d_2 = d'_2$. Ainsi, d'après a) et b), l'application $(d_1, d_2) \mapsto d_1 d_2$ est une bijection des couples (diviseur de a , diviseur de b) sur les diviseurs de ab , et

$$\sigma(ab) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} d_1 d_2 = \left(\sum_{d_1 \mid a} d_1 \right) \left(\sum_{d_2 \mid b} d_2 \right) = \sigma(a) \sigma(b).$$

3. $M \geq 3$ est premier impair, donc $2^{k-1} \wedge M = 1$ et

$$\sigma(n) = \sigma(2^{k-1}) \sigma(M) = (2^k - 1)(M + 1) = M \times 2^k = 2n : \quad n \text{ est parfait.}$$

$k = 2, 3, 5, 7$ donnent $M = 3, 7, 31, 127$ (premiers), tandis que $2^4 - 1 = 15$ et $2^6 - 1 = 63$ ne le sont pas : 6, 28, 496, 8128.

4. a) $1 + 2 + \dots + M = \frac{M(M+1)}{2} = \frac{M \times 2^k}{2} = 2^{k-1} M = n.$

b) k impair, donc $k \equiv 1, 3$ ou 5 [6], et les puissances de 2 modulo 9 sont 6-périodiques :

k [6]	2^{k-1} [9]	$M = 2^k - 1$ [9]	n [9]
1	1	1	1
3	4	7	$28 \equiv 1$
5	$16 \equiv 7$	$31 \equiv 4$	$28 \equiv 1$

Donc $n \equiv 1$ [9] : par exemple $496 = 9 \times 55 + 1$ et $8128 = 9 \times 903 + 1$.

c) k est premier. Si $k = 2$, $n = 6$. Sinon k est impair : $k \equiv 1$ ou 3 [4]. Modulo 10, $2^4 \equiv 6$ et $6^2 \equiv 6$, donc $2^{4j} \equiv 6$ pour $j \geq 1$.

– Si $k \equiv 1$ [4] ($k \geq 5$) : $2^{k-1} \equiv 6$, $2^k \equiv 12 \equiv 2$, $M \equiv 1$ et $n \equiv 6$ [10].

– Si $k \equiv 3$ [4] : $2^{k-1} \equiv 4 \times 2^{4j} \equiv 4$ (y compris pour $j = 0$), $2^k \equiv 8$, $M \equiv 7$ et $n \equiv 28 \equiv 8$ [10].

Le chiffre des unités de n est donc **6 ou 8** (6, 28, 496, 8128 ✓).

33 Corrigés : équations diophantiennes

■ Corrigé de l'exercice 55

1. On lit les points $(-6, -3)$, $(-1, -1)$, $(4, 1)$ et $(9, 3)$. On passe de l'un au suivant par le vecteur $\vec{u}(5, 2)$; deux points consécutifs sont distants de $\|\vec{u}\| = \sqrt{25 + 4} = \sqrt{29}$.

2. $2 \times 4 - 5 \times 1 = 3$: le couple $(4, 1)$ est solution. Alors

$$2x - 5y = 3 \iff 2x - 5y = 2 \times 4 - 5 \times 1 \iff 2(x - 4) = 5(y - 1).$$

Donc $5 \mid 2(x - 4)$ et $5 \wedge 2 = 1$: par le théorème de Gauss, $5 \mid x - 4$, soit $x = 4 + 5k$ ($k \in \mathbb{Z}$) ; en reportant, $10k = 5(y - 1)$, d'où $y = 1 + 2k$. Réciproquement $2(4 + 5k) - 5(1 + 2k) = 3$ ✓.

$$S = \{(4 + 5k, 1 + 2k) : k \in \mathbb{Z}\}.$$

3. $-50 \leq 4 + 5k \leq 50 \iff -\frac{54}{5} \leq k \leq \frac{46}{5} \iff -10 \leq k \leq 9$; pour ces valeurs, $y = 1 + 2k \in [-19, 19] \subset [-50, 50]$. Il y a donc 20 points.

4. Pour $M_k(4 + 5k, 1 + 2k)$: $OM_k^2 = (4 + 5k)^2 + (1 + 2k)^2 = 29k^2 + 44k + 17 = k(29k + 44) + 17$. Si $k \geq 0$, $OM_k^2 \geq 17$; si $k \leq -2$, $29k + 44 \leq -14$ et $k(29k + 44) \geq 28$, donc $OM_k^2 \geq 45$; enfin $OM_{-1}^2 = 2$. Le point cherché est $M_{-1}(-1, -1)$, à la distance $\sqrt{2}$ de O .

■ Corrigé de l'exercice 56

- $120 = 2^3 \times 3 \times 5$ et $75 = 3 \times 5^2$, donc $120 \wedge 75 = \boxed{15}$. Comme $1995 = 15 \times 133$, en divisant par 15 : $120x + 75y = 1995 \iff 8x + 5y = 133$.
- $8 + 125 = 133$ ✓. Puis $8x + 5y = 8 \times 1 + 5 \times 25 \iff 8(x - 1) = 5(25 - y)$; $5 \mid 8(x - 1)$ et $5 \wedge 8 = 1$, donc $x = 1 + 5k$, puis $y = 25 - 8k$: $S = \{(1 + 5k, 25 - 8k) : k \in \mathbb{Z}\}$.
- $x \geq 0 \iff k \geq -\frac{1}{5} \iff k \geq 0$ et $y \geq 0 \iff k \leq \frac{25}{8} \iff k \leq 3$. Quatre possibilités :
 $(x, y) \in \{(1, 25), (6, 17), (11, 9), (16, 1)\}$.
- $x \geq y$ pour $(11, 9)$ et $(16, 1)$ seulement, avec 20 et 17 articles : le club achète **11 ballons et 9 maillots**.
- $120x + 75y$ est toujours un multiple de 15, or $1990 = 15 \times 132 + 10$ n'en est pas un : la facture est fausse.

■ Corrigé de l'exercice 57

- $77 = 7 \times 11$ et $105 = 3 \times 5 \times 7$, donc $77 \wedge 105 = \boxed{7}$ et $(E) \iff 7(11x - 15y) = 7 \times 4 \iff 11x - 15y = 4$.
 - $11 \times 14 - 15 \times 10 = 154 - 150 = 4$ ✓. Alors $(E) \iff 11(x - 14) = 15(y - 10)$; $15 \mid 11(x - 14)$ et $15 \wedge 11 = 1$, donc (Gauss) $x = 14 + 15k$, puis $y = 10 + 11k$: $S = \{(14 + 15k, 10 + 11k) : k \in \mathbb{Z}\}$.
- δ divise x et y , donc $11x - 15y = 4$: $\delta \in \{1, 2, 4\}$.
 - $x \equiv k [2]$ et $y \equiv k [2]$.
 – Si k est impair, x et y sont impairs : $\boxed{\delta = 1}$ (ex. $k = 1$: $(29, 21)$).
 – Si $k = 2m$: $x = 2(7 + 15m)$ et $y = 2(5 + 11m)$, avec $7 + 15m \equiv 5 + 11m \equiv m + 1 [2]$. Si m est impair ($k \equiv 2 [4]$), 4 divise x et y : $\boxed{\delta = 4}$ (ex. $k = 2$: $(44, 32)$) ; si m est pair ($k \equiv 0 [4]$), $\frac{x}{2}$ et $\frac{y}{2}$ sont impairs : $\boxed{\delta = 2}$ (ex. $k = 0$: $(14, 10)$).
- $77x \equiv 28 [105] \iff \exists y \in \mathbb{Z}, 77x - 28 = 105y \iff \exists y \in \mathbb{Z}, (x, y)$ solution de $(E) \iff \boxed{x \equiv 14 [15]}$.
- $n \equiv 2 [11]$ et $n \equiv 6 [15] \iff$ il existe $(x, y) \in \mathbb{Z}^2$ tel que $n = 11x + 2 = 15y + 6 \iff n = 11x + 2$ avec $11x - 15y = 4$. D'après 1.b), $x = 14 + 15k$, donc $n = 11(14 + 15k) + 2 = 156 + 165k$:
 $\boxed{n \equiv 156 [165]}$ (contrôle : $156 = 11 \times 14 + 2 = 15 \times 10 + 6$ ✓).
 - $156 + 165k > 2026 \iff k > \frac{1870}{165} \approx 11,3$: $k = 12$ et $n = \boxed{2136}$ ($= 11 \times 194 + 2 = 15 \times 142 + 6$).

■ Corrigé de l'exercice 58

- $(2x + 5)(2y - 3) = 4xy - 6x + 10y - 15 = 2(2xy - 3x + 5y) - 15$.
 - L'équation équivaut à $(2x + 5)(2y - 3) = 2 \times 22 - 15 = 29$, nombre premier. Donc $2x + 5 \in \{1, -1, 29, -29\}$ et $2y - 3 = \frac{29}{2x+5}$:

$2x + 5$	1	-1	29	-29
$2y - 3$	29	-29	1	-1
(x, y)	$(-2, 16)$	$(-3, -13)$	$(12, 2)$	$(-17, 1)$

Les quatre couples sont entiers : $S = \{(-2, 16), (-3, -13), (12, 2), (-17, 1)\}$.

2. $x^2 - xy - 2y^2 = x^2 + xy - 2xy - 2y^2 = (x - 2y)(x + y)$. On pose $u = x - 2y$ et $v = x + y$; alors $uv = 7$, et $x = \frac{u+2v}{3}$, $y = \frac{v-u}{3}$:

$$(u, v) = (1, 7) \rightarrow (5, 2), \quad (7, 1) \rightarrow (3, -2), \quad (-1, -7) \rightarrow (-5, -2), \quad (-7, -1) \rightarrow (-3, 2).$$

Ces quatre couples sont entiers : $S = \{(5, 2), (3, -2), (-5, -2), (-3, 2)\}$.

3. a) L'aire $\frac{ab}{2}$ est égale au périmètre $a+b+c$, donc $c = \frac{ab}{2} - a - b$. En élevant au carré, avec $c^2 = a^2 + b^2$:

$$\frac{a^2 b^2}{4} - ab(a+b) + (a+b)^2 = a^2 + b^2 \iff \frac{a^2 b^2}{4} - ab(a+b) + 2ab = 0 \iff ab - 4(a+b) + 8 = 0,$$

en divisant par $\frac{ab}{4} > 0$. Comme $(a-4)(b-4) = ab - 4a - 4b + 16$, on obtient $(a-4)(b-4) = 8$.

b) Si $a \leq 4$: $a = 4$ donne $0 \neq 8$, et $a \in \{1, 2, 3\}$ donne $b-4 \in \{-\frac{8}{3}, -4, -8\}$, donc $b \notin \mathbb{N}^*$. Ainsi $1 \leq a-4 \leq b-4$ et $(a-4, b-4) \in \{(1, 8), (2, 4)\}$: $(a, b) = (5, 12)$ ou $(6, 8)$, puis $c = 30 - 17 = 13$ ou $c = 24 - 14 = 10$. Réciproquement $5^2 + 12^2 = 13^2$ avec aire et périmètre égaux à 30, et $6^2 + 8^2 = 10^2$ avec aire et périmètre égaux à 24 : **les triangles (5, 12, 13) et (6, 8, 10)**.

■ Corrigé de l'exercice 59

1. $6 \wedge 10 = 2$, $6 \wedge 15 = 3$, $10 \wedge 15 = 5$. $6x + 10y$ est pair, $6x + 15z$ multiple de 3 et $10y + 15z$ multiple de 5 : aucune de ces trois équations n'a de solution (aucun de ces PGCD ne divise 1). Pourtant $6 + 10 - 15 = 1$: $(1, 1, -1)$ est solution de (E).
2. a) $15z = 1 - 6x - 10y$ est impair, donc z est impair. Avec $z = 1 + 2t$: $6x + 10y = 1 - 15 - 30t$, soit, en divisant par 2, $3x + 5y = -7 - 15t$.
- b) $3(-4 - 5t) + 5 \times 1 = -7 - 15t$, donc $3(x + 4 + 5t) = 5(1 - y)$. Par Gauss ($3 \wedge 5 = 1$) : $x + 4 + 5t = 5s$ avec $s \in \mathbb{Z}$, puis $15s = 5(1 - y)$, soit $y = 1 - 3s$. Réciproquement : $6(-4 + 5s - 5t) + 10(1 - 3s) + 15(1 + 2t) = -24 + 10 + 15 = 1$ ✓. Ainsi

$$S = \{(-4 + 5s - 5t, 1 - 3s, 1 + 2t) : (s, t) \in \mathbb{Z}^2\} \quad (s = 0, t = -1 \text{ redonne } (1, 1, -1)).$$

3. a) Si $6x + 10y + 15z = 29$ avec $x, y, z \in \mathbb{N}$: z est impair et $15z \leq 29$, donc $z = 1$ et $3x + 5y = 7$; alors $y \in \{0, 1\}$, et $3x = 7$ ou $3x = 2$: impossible. **29 n'est pas représentable.**
- b) $30 = 2 \times 15$, $31 = 6 + 10 + 15$, $32 = 2 \times 6 + 2 \times 10$, $33 = 3 \times 6 + 15$, $34 = 4 \times 6 + 10$, $35 = 2 \times 10 + 15$. Si $n \geq 30$, on écrit $n - 30 = 6q + r$ avec $0 \leq r \leq 5$: $n = (30 + r) + 6q$ s'obtient en ajoutant q fois 6 à une représentation de $30 + r$. **Tout entier $n \geq 30$ est représentable** : 29 est le plus grand entier non représentable.

■ Corrigé de l'exercice 60

1. a) *Existence*. Par Bézout, $au + bv = 1$, donc $n = a(nu) + b(nv)$. On divise nu par b : $nu = bq + x$ avec $0 \leq x \leq b - 1$, et $n = ax + b(nv + aq)$.
- Unicité*. Si $ax + by = ax' + by'$ avec $x, x' \in \{0, \dots, b - 1\}$, alors $a(x - x') = b(y' - y)$: $b \mid a(x - x')$ et $a \wedge b = 1$, donc $b \mid x - x'$ (Gauss) ; comme $|x - x'| \leq b - 1$, $x = x'$, puis $y = y'$.
- b) Si $y \geq 0$, $(x, y) \in \mathbb{N}^2$ convient. Réciproquement, si $n = ax' + by'$ avec $x', y' \in \mathbb{N}$, on écrit $x' = bq + x$ ($q \in \mathbb{N}$, $0 \leq x \leq b - 1$) : $n = ax + b(y' + aq)$, et par unicité $y = y' + aq \geq 0$.

2. $g = a(b-1) + b \times (-1)$ avec $0 \leq b-1 \leq b-1$: c'est l'écriture de 1.a), avec $y = -1 < 0$, donc g **n'est pas affranchissable**. Si $n > g$ s'écrit $n = ax + by$ comme en 1.a) avec $y \leq -1$, alors $n \leq a(b-1) - b = g$: contradiction. Donc $y \geq 0$ et **tout $n > g$ est affranchissable**.
3. a) Si $n = ax + by$ (écriture de 1.a)), alors $g - n = a(b-1-x) + b(-1-y)$ avec $0 \leq b-1-x \leq b-1$: c'est l'écriture de $g - n \in \mathbb{N}$. Ainsi n affranchissable $\iff y \geq 0 \iff -1-y < 0 \iff g - n$ non affranchissable.
- b) D'après 2, les montants non affranchissables sont dans $\{0, \dots, g\}$. La bijection $n \mapsto g - n$ de $\{0, \dots, g\}$ sur lui-même échange affranchissables et non affranchissables : ils sont aussi nombreux, donc il y a $\frac{g+1}{2} = \frac{ab-a-b+1}{2} = \frac{(a-1)(b-1)}{2}$ montants non affranchissables.
4. $a = 5, b = 9$: $g = 45 - 14 = 31$ et il y a $\frac{4 \times 8}{2} = 16$ montants non affranchissables : 1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 16, 17, 21, 22, 26, 31.

Dans le tableau ci-dessous (colonnes : restes modulo 9), la colonne r devient affranchissable à partir du plus petit multiple de 5 congru à r modulo 9 : pour $r = 0, \dots, 8$, ce sont 0, 10, 20, 30, 40 (hors tableau), 5, 15, 25, 35.

0	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

vert : affranchissable
rouge : non affranchissable

34

Corrigés : défis de concours

■ Corrigé de l'exercice 61

1. a) p premier et $1 \leq a \leq p-1$, donc $a \wedge p = 1$: par Bézout, $au + pv = 1$, d'où $au \equiv 1 [p]$. Le reste a' de u modulo p vérifie $aa' \equiv 1 [p]$, et $a' \neq 0$ (sinon $0 \equiv 1$). Si $aa' \equiv aa'' \equiv 1 [p]$ avec $a', a'' \in \{1, \dots, p-1\}$, alors $p \mid a(a' - a'')$, donc $p \mid a' - a''$ (Gauss) et, comme $|a' - a''| < p$, $a' = a''$.
- b) $a' = a \iff a^2 \equiv 1 [p] \iff p \mid (a-1)(a+1) \iff p \mid a-1$ ou $p \mid a+1$ (lemme d'Euclide). Comme $0 \leq a-1 \leq p-2$ et $2 \leq a+1 \leq p$: $a = 1$ ou $a = p-1$.
2. Pour $p = 2$ et $p = 3$: $1! = 1 \equiv -1 [2]$ et $2! = 2 \equiv -1 [3]$. Soit $p \geq 5$. L'application $a \mapsto a'$ est involutive (a est l'inverse de a') et envoie $\{2, \dots, p-2\}$ dans lui-même (si $a' = 1$ ou $p-1$, alors $a = 1$ ou $p-1$). D'après 1.b), elle n'a pas de point fixe dans cet ensemble : ses éléments se regroupent en paires $\{a, a'\}$ de produit $\equiv 1 [p]$. Donc $2 \times 3 \times \dots \times (p-2) \equiv 1 [p]$ et
- $$(p-1)! \equiv 1 \times 1 \times (p-1) \equiv -1 [p].$$
3. $n = de$ avec $1 < d < n$: $d \leq n-1$, donc $d \mid (n-1)!$. Si l'on avait $n \mid (n-1)! + 1$, alors $d \mid (n-1)! + 1$, d'où $d \mid 1$: absurde. Avec le théorème de Wilson : $n \geq 2$ est premier $\iff n \mid (n-1)! + 1$.
4. $100! \equiv -1 [101]$ et $100! = 97! \times 98 \times 99 \times 100 \equiv 97! \times (-3)(-2)(-1) = -6 \times 97! [101]$. Donc $6 \times 97! \equiv 1 [101]$. Comme $6 \times 17 = 102 \equiv 1 [101]$, on multiplie par 17 : $97! \equiv 17 [101]$: le reste est $\boxed{17}$.
5. a) Les entiers $1, \dots, 4m$ se regroupent en couples $\{j, p-j\}$, $1 \leq j \leq 2m$, et $p-j \equiv -j [p]$:

$$(p-1)! = \prod_{j=1}^{2m} j(p-j) \equiv \prod_{j=1}^{2m} (-j^2) = (-1)^{2m} ((2m)!)^2 = ((2m)!)^2 [p],$$

donc, par Wilson, $((2m)!)^2 \equiv -1 [p] : -1$ est un carré modulo p .

b) $p = 13, m = 3 : 6! = 720 = 13 \times 55 + 5$, donc $5^2 \equiv -1 [13]$ ($25 = 26 - 1$ ✓). Alors $x^2 \equiv -1 \iff x^2 \equiv 5^2 \iff 13 \mid (x-5)(x+5) \iff x \equiv \pm 5 [13] : x \in \{5, 8\}$.

Avec l'exercice 20 : pour p premier impair, -1 est un carré modulo p si et seulement si $p \equiv 1 [4]$.

■ Corrigé de l'exercice 62

1. $(ac - bd)^2 + (ad + bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = (a^2 + b^2)(c^2 + d^2)$ (les doubles produits $\mp 2abcd$ s'éliminent). Donc S est stable par produit. Avec $13 = 2^2 + 3^2$ et $17 = 1^2 + 4^2 = 4^2 + 1^2$:

$$221 = (2 - 12)^2 + (8 + 3)^2 = 10^2 + 11^2 \quad \text{et} \quad 221 = (8 - 3)^2 + (2 + 12)^2 = 5^2 + 14^2.$$

2. a) Supposons $p \nmid b$: b a un inverse b' modulo p (exercice 61). De $a^2 \equiv -b^2 [p]$ on tire $(ab')^2 \equiv -(bb')^2 \equiv -1 [p]$: contradiction. Donc $p \mid b$, puis $p \mid a^2$ et $p \mid a$ (Euclide).

b) Récurrence forte sur l'exposant v de p dans $n = a^2 + b^2$. Si $v = 0$, il est pair. Si $v \geq 1$, $p \mid a$ et $p \mid b$ d'après a), donc $p^2 \mid n$ et $\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2 \in S$ est non nul, d'exposant $v - 2 \geq 0$, pair par hypothèse de récurrence : v est pair.

$2001 = 3 \times 23 \times 29$: l'exposant de 3 (premier, $\equiv 3 [4]$) vaut 1, donc $2001 \notin S$ (l'argument modulo 4 ne suffisait pas : $2001 \equiv 1 [4]$).

3. a) $q + 1 > \sqrt{p}$, donc $(q + 1)^2 > p$: il y a plus d'entiers $x - my$ que de restes possibles modulo p . D'après le principe des tiroirs, deux de ces entiers, associés à des couples distincts, ont le même reste.

b) $x_1 - my_1 \equiv x_2 - my_2 [p]$ donne $a \equiv mb$, puis $a^2 \equiv m^2b^2 \equiv -b^2 [p] : p \mid a^2 + b^2$. Comme $(a, b) \neq (0, 0)$, $|a| \leq q$, $|b| \leq q$ et $q^2 < p$ (p premier n'est pas un carré) : $0 < a^2 + b^2 \leq 2q^2 < 2p$. Le seul multiple de p dans $]0, 2p[$ est p : $p = a^2 + b^2 \in S$.

4. $12^2 = 144 = 5 \times 29 - 1$ ✓, et $q = E(\sqrt{29}) = 5$. Les couples $(0, 2)$ et $(5, 0)$ donnent $0 - 24 = -24$ et 5, de même reste 5 modulo 29 : $a = -5, b = 2$, et $29 = 5^2 + 2^2$. (En pratique : on cherche $b \in \{1, \dots, 5\}$ tel que $12b$ soit congru modulo 29 à un entier de $[-5, 5]$; $b = 2$ donne $24 \equiv -5$, et $b = 5$ donne $60 \equiv 2$, soit la même écriture $29 = 2^2 + 5^2$.)

$2029 - 45^2 = 4$: $2029 = 45^2 + 2^2$. Avec $13 = 2^2 + 3^2$ et l'identité de la question 1 :

$$13 \times 2029 = 26377 = (2 \times 45 - 3 \times 2)^2 + (2 \times 2 + 3 \times 45)^2 = 84^2 + 139^2,$$

$$13 \times 2029 = (2 \times 2 - 3 \times 45)^2 + (2 \times 45 + 3 \times 2)^2 = 131^2 + 96^2.$$

■ Corrigé de l'exercice 63

1. Les entiers de $\{1, \dots, 12\}$ premiers avec 12 sont 1, 5, 7, 11 : $\varphi(12) = 4$. Pour p premier, seul p n'est pas premier avec p : $\varphi(p) = p - 1$. Enfin $k \wedge p^\alpha \neq 1 \iff p \mid k$ (p est le seul diviseur premier de p^α) ; il y a $p^{\alpha-1}$ multiples de p dans $\{1, \dots, p^\alpha\}$, donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
2. a) $a \wedge n = 1$ et $r_i \wedge n = 1$, donc $ar_i \wedge n = 1$ (cours) ; un diviseur commun à s_i et n divise ar_i , donc $s_i \wedge n = 1$ (en particulier $s_i \neq 0$, et $s_i \in \{1, \dots, n-1\}$). Si $s_i = s_j$, alors $n \mid a(r_i - r_j)$, donc $n \mid r_i - r_j$ (Gauss), et $|r_i - r_j| < n$ donne $i = j$.

b) Les s_i sont N éléments distincts de l'ensemble $\{r_1, \dots, r_N\}$, qui a N éléments : ils le décrivent tout entier. En notant $R = r_1 \cdots r_N$:

$$R = s_1 \cdots s_N \equiv (ar_1) \cdots (ar_N) = a^N R [n],$$

donc $n \mid (a^N - 1)R$; comme $R \wedge n = 1$, Gauss donne $a^{\varphi(n)} \equiv 1 [n]$. Pour $n = p$ premier, $\varphi(p) = p - 1$: c'est le petit théorème de Fermat.

3. a) $1000 = 2^3 \times 5^3$, donc $k \wedge 1000 = 1 \iff 2 \nmid k \text{ et } 5 \nmid k$. Dans $\{1, \dots, 1000\}$, il y a 500 multiples de 2, 200 de 5 et 100 de 10 : $500 + 200 - 100 = 600$ entiers sont divisibles par 2 ou par 5, et $\varphi(1000) = 1000 - 600 = 400$.

b) $11 \wedge 1000 = 1$, donc $11^{400} \equiv 1 [1000]$; comme $2026 = 5 \times 400 + 26$, $11^{2026} \equiv 11^{26} [1000]$. Par la formule du binôme, les termes en 10^k avec $k \geq 3$ sont multiples de 1000 :

$$11^{26} = (10 + 1)^{26} \equiv 1 + 26 \times 10 + \binom{26}{2} \times 100 = 1 + 260 + 32500 = 32761 \equiv 761 [1000].$$

Les trois derniers chiffres de 11^{2026} sont 761.

4. De même $\varphi(100) = 100 - (50 + 20 - 10) = 40$ et $\varphi(40) = 40 - (20 + 8 - 4) = 16$. Par Euler, $3^{16} \equiv 1 [40]$; comme $2026 = 16 \times 126 + 10$ et $3^4 = 81 \equiv 1 [40]$: $3^{2026} \equiv 3^{10} = (3^4)^2 \times 9 \equiv 9 [40]$. Ainsi $3^{2026} = 40Q + 9$ et, par Euler ($3 \wedge 100 = 1$) :

$$3^{3^{2026}} = (3^{40})^Q \times 3^9 \equiv 3^9 = 19683 \equiv 83 [100] : \text{ les deux derniers chiffres sont } 83.$$

■ Corrigé de l'exercice 64

- Si $p \mid a$, les deux membres sont divisibles par p . Sinon, Fermat donne $a^{p-1} \equiv 1 [p]$; avec $n - 1 = (p - 1)t$ ($t \in \mathbb{N}^*$), $a^{n-1} = (a^{p-1})^t \equiv 1$, donc $a^n \equiv a [p]$.
- D'après 1, chaque p_i divise $a^n - a$. Les p_i sont des nombres premiers distincts, donc premiers entre eux deux à deux : leur produit n divise $a^n - a$ (corollaire de Gauss, par récurrence). Comme $k \geq 2$, n n'est pas premier : c'est un nombre de Carmichael.
- On applique le critère de Korselt :

n	décomposition	$n - 1$
561	$3 \times 11 \times 17$	$560 = 2 \times 280 = 10 \times 56 = 16 \times 35$
1105	$5 \times 13 \times 17$	$1104 = 4 \times 276 = 12 \times 92 = 16 \times 69$
1729	$7 \times 13 \times 19$	$1728 = 6 \times 288 = 12 \times 144 = 18 \times 96$

4. Avec $a = n - 1 \equiv -1 : (-1)^n \equiv -1 [n]$. Si n était pair : $1 \equiv -1 [n]$, $n \mid 2$, $n = 2$, qui est premier : exclu. **n est impair.**

Si $p^2 \mid n$ (p premier), avec $a = p : p^n \equiv p [n]$, donc $p^n \equiv p [p^2]$; or $n \geq 2$, donc $p^2 \mid p^n$, d'où $p^2 \mid p$: absurde. **n est sans facteur carré.**

5. $(6k + 1)(12k + 1) = 72k^2 + 18k + 1$, puis $n = 1296k^3 + 396k^2 + 36k + 1$, donc

$$n - 1 = 36k(36k^2 + 11k + 1)$$

est divisible par $6k$, $12k$ et $18k$. Le critère de Korselt (trois premiers distincts) conclut. $k = 1 : 7 \times 13 \times 19 = 1729$; $k = 6 : 37, 73, 109$ sont premiers et $37 \times 73 \times 109 = 294409$ est un nombre de Carmichael.

■ Corrigé de l'exercice 65

- Si $b = 0$: $2^a = 2$, $a = 1$. Si $b \geq 1$: $2^a = 1 + 3^b \equiv 1 \pmod{3}$ et $2 \equiv -1 \pmod{3}$, donc a est pair : $a = 2c$ ($c \geq 1$). Alors $(2^c - 1)(2^c + 1) = 3^b$: par unicité de la décomposition, les deux facteurs sont des puissances de 3 ; ils diffèrent de 2, donc ne sont pas tous deux multiples de 3 : $2^c - 1 = 1$, $c = 1$, $a = 2$ et $b = 1$. $(a, b) \in \{(1, 0), (2, 1)\}$.
- Si $a = 0$: $3^b = 2$, impossible ; si $a = 1$: $b = 1$. Si $a \geq 2$: $3^b = 1 + 2^a \equiv 1 \pmod{4}$ et $3 \equiv -1 \pmod{4}$, donc $b = 2c$ ($c \geq 1$) et $(3^c - 1)(3^c + 1) = 2^a$: deux puissances de 2 qui diffèrent de 2. Si $2^u - 2^v = 2$ avec $u > v$: $v = 0$ donne $2^u = 3$, $v \geq 2$ rend le membre de gauche multiple de 4 ; donc $v = 1$, $u = 2$, soit $3^c - 1 = 2$: $c = 1$, $b = 2$, $2^a = 8$, $a = 3$. $(a, b) \in \{(1, 1), (3, 2)\}$.
- a) $1 + 2 + \dots + 2^n = 2^{n+1} - 1 = 3^b \iff 2^{n+1} - 3^b = 1 \iff (n+1, b) \in \{(1, 0), (2, 1)\}$: $n \in \{0, 1\}$ (sommes $1 = 3^0$ et $3 = 3^1$).
b) $1 + 3 + \dots + 3^n = \frac{3^{n+1} - 1}{2} = 2^a \iff 3^{n+1} - 2^{a+1} = 1 \iff (a+1, n+1) \in \{(1, 1), (3, 2)\}$: $n \in \{0, 1\}$ (sommes $1 = 2^0$ et $4 = 2^2$).
- Si $b = 0$: $2^a = 8$, $a = 3$. Si $b \geq 1$: $2^a \equiv 7 \equiv 1 \pmod{3}$, donc a est pair ; de plus $2^a = 7 + 3^b \geq 10$, donc $a \geq 4$ et $8 \mid 2^a$, d'où $3^b \equiv -7 \equiv 1 \pmod{8}$. Or $3^b \equiv 3$ ou $1 \pmod{8}$ selon que b est impair ou pair : b est pair. Avec $a = 2c$, $b = 2d$:

$$(2^c - 3^d)(2^c + 3^d) = 7, \quad 0 < 2^c - 3^d < 2^c + 3^d,$$
donc $2^c - 3^d = 1$ et $2^c + 3^d = 7$: $2^c = 4$, $3^d = 3$, soit $(a, b) = (4, 2)$. $(a, b) \in \{(3, 0), (4, 2)\}$ ($8 - 1 = 16 - 9 = 7$ ✓).

■ Corrigé de l'exercice 66

- a) Un nombre premier divisant m_k et $m_1 \dots m_{k-1}$ diviserait l'un des m_i ($i < k$) par le lemme d'Euclide, alors que $m_k \wedge m_i = 1$. Donc $m_k \wedge (m_1 \dots m_{k-1}) = 1$.
b) Cas $k = 2$. Bézout : $m_1 u + m_2 v = 1$. Posons $x_0 = r_1 m_2 v + r_2 m_1 u$: $x_0 \equiv r_1 m_2 v = r_1 (1 - m_1 u) \equiv r_1 \pmod{m_1}$ et de même $x_0 \equiv r_2 \pmod{m_2}$. Si x est solution, m_1 et m_2 divisent $x - x_0$, donc $m_1 m_2 \mid x - x_0$ (corollaire de Gauss) ; réciproquement, tout $x \equiv x_0 \pmod{m_1 m_2}$ convient. *Hérédité.* Si le résultat vaut pour $k-1$ modules, les $k-1$ premières congruences équivalent à $x \equiv y_0 \pmod{M'}$, avec $M' = m_1 \dots m_{k-1}$; comme $M' \wedge m_k = 1$ (a), le cas $k = 2$ appliqué à $x \equiv y_0 \pmod{M'}$, $x \equiv r_k \pmod{m_k}$ donne exactement une classe modulo $M' m_k = M$.
- Le système s'écrit $n \equiv 0 \pmod{4}$, $n \equiv 8 \pmod{9}$, $n \equiv 23 \pmod{25}$ (modules premiers entre eux deux à deux) : une seule classe modulo 900. On écrit $n = 25t + 23$: $4 \mid n \iff t + 3 \equiv 0 \pmod{4} \iff t \equiv 1 \pmod{4}$, soit $n \equiv 48 \pmod{100}$. Puis $n = 48 + 100s \equiv 3 + s \pmod{9}$: $n \equiv 8 \pmod{9} \iff s \equiv 5 \pmod{9}$. Donc $n \equiv 548 \pmod{900}$ et le plus petit est $n = 548$: $548 = 4 \times 137$, $549 = 9 \times 61$, $550 = 25 \times 22$ ✓.
- Soit $p_1, \dots, p_k$ des nombres premiers distincts : les p_i^2 sont premiers entre eux deux à deux. D'après 1, il existe n tel que $n \equiv -i \pmod{p_i^2}$ pour $1 \leq i \leq k$, et, quitte à ajouter un multiple de $p_1^2 \dots p_k^2$, $n \in \mathbb{N}$. Alors $p_i^2 \mid n + i$: les k entiers consécutifs $n + 1, \dots, n + k$ conviennent.
- Soit $p_1, q_1, \dots, p_k, q_k$ des nombres premiers deux à deux distincts ; les $p_i q_i$ sont premiers entre eux deux à deux. Il existe $n \in \mathbb{N}$ tel que $n \equiv -i \pmod{p_i q_i}$ pour $1 \leq i \leq k$. Alors $n + i > 0$ est divisible par les deux nombres premiers distincts p_i et q_i : ce n'est pas une puissance p^α d'un nombre premier (dont p est le seul diviseur premier, et $n + i \geq p_i q_i \geq 6 > 1$). Les entiers $n + 1, \dots, n + k$ conviennent.

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 · Division euclidienne	31 à 36	/ 6	
Thème B · Congruences et restes	37 à 42	/ 6	
Thème C · PGCD et théorème de Bézout	43 à 48	/ 6	
Thème D · Gauss et nombres premiers	49 à 54	/ 6	
Thème E · Équations diophantiennes	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 intégral

Maths Olympiad