BURHAN

Arithmétique dans $\mathbb{Z}$

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

Version en ligne : burhan.ma/2bac/sciences-mathematiques/mathematiques/arithmetique-dans-z/cours

Chapitre	Semestre
Arithmétique dans $\mathbb{Z}$	Semestre 2

Ce que cache un entier

Prends un entier impair, élève-le au carré, puis retire 1. Avec 3, tu obtiens 8. Avec 5, tu obtiens 24. Avec 7, c'est 48 ; avec 11, c'est 120.

Tous ces nombres sont des multiples de 8. Hasard des petits nombres, ou loi cachée ?

Devine : Un impair au carré

Soit n un entier impair. Selon toi, que vaut le reste de la division de $n^2 - 1$ par 8 ?

A. Il vaut 0 seulement quand n est premier.

Faux.
Essaie $n = 9$: $81 - 1 = 80 = 8 \times 10$. Le reste est nul, alors que 9 n'est pas premier.

B. Il vaut 0 pour tout entier impair n.

Juste.
C'est bien une loi : tout entier impair n vérifie $8 \mid n^2 - 1$. Les congruences la prouvent en quelques lignes.

C. Il finit par ne plus valoir 0 pour un n assez grand.

Faux.
Aucun contre-exemple n'existe, même très grand. Mais seule une preuve permet de l'affirmer.

Indice 1
Regarde le reste de n dans la division par 8 : il est impair.
Indice 2
Écris $n = 8m + r$, avec r impair et $0 \leq r < 8$, puis développe $n^2 - 1$.

Correction
Le reste vaut toujours 0. Soit n un entier impair. Dans la division euclidienne de n par 8, le reste est impair : n s'écrit $8m + 1$, $8m + 3$, $8m + 5$ ou $8m + 7$, avec m entier.

En développant, $n^2 - 1$ vaut respectivement $8(8m^2 + 2m)$, $8(8m^2 + 6m + 1)$, $8(8m^2 + 10m + 3)$ ou $8(8m^2 + 14m + 6)$.

Conclusion. C'est un multiple de 8 dans chaque cas : pour tout entier impair n, $8 \mid n^2 - 1$.

Méfie-toi des essais : $n^2 + n + 41$ est premier pour $n = 0, 1, \ldots, 39$. Pourtant, pour $n = 40$, il vaut $1681 = 41 \times 41$.

Observer ne prouve donc rien. Dans ce chapitre, tu vas apprendre à **prouver** des propriétés des entiers. La question de l'impair au carré, tu sauras la trancher et la rédiger avec les congruences.

Divisibilité et division euclidienne

Diviser dans les entiers relatifs

Vérifie : Qui divise qui ?

Tu connais la divisibilité depuis la 1BAC ; en 2BAC, chaque propriété sera **prouvée**. Laquelle de ces affirmations est vraie ?

A. $4 \mid 2$

Faux.
Le sens est inversé : c'est 2 qui divise 4. Pour avoir $4 \mid 2$, il faudrait un entier k tel que $2 = 4k$.

B. $-6 \mid 42$

Juste.
On a $42 = (-7) \times (-6)$, avec $-7 \in \mathbb{Z}$. Un diviseur peut être négatif.

C. $0 \mid 7$

Faux.
Tout multiple de 0 vaut 0 : aucun entier k ne vérifie $7 = k \times 0$.

Indice 1
Traduis $a \mid b$ par : il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Correction
Seule l'affirmation $-6 \mid 42$ est vraie, car $42 = (-7) \times (-6)$. Dans $a \mid b$, on cherche b comme multiple de a : l'ordre compte.

Définition : Divisibilité dans $\mathbb{Z}$

Soient a et b deux entiers relatifs. On dit que a **divise** b, et on écrit $a \mid b$, s'il existe un entier relatif k tel que $b = ka$. On dit aussi que a est un **diviseur** de b, ou que b est un **multiple** de a. Dans le cas contraire, on écrit $a \nmid b$.

Exemple : Trois cas à lire

- $-9 \mid 63$, car $63 = (-7) \times (-9)$.
- $13 \nmid 50$: les multiples de 13 voisins de 50 sont 39 et 52.
- 1 et -1 divisent tout entier. Tout entier divise 0, car $0 = 0 \times a$.

Combiner des divisibilités

On sait que $7 \mid 91$ et $7 \mid 35$. Alors 7 divise $91 - 35 = 56$. Il divise aussi $2 \times 91 + 3 \times 35 = 287 = 7 \times 41$.

Pourquoi est-ce vrai ? Chaque terme est un multiple de 7, donc leur combinaison aussi. La propriété suivante le dit pour tous les entiers, avec sa preuve.

Propriété : Propriétés de la divisibilité

Soient a, b et c des entiers relatifs.

1. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.
2. Si $a \mid b$ et $a \mid c$, alors $a \mid b\lambda + c\mu$ pour tous entiers relatifs λ et μ.
3. Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$.
4. Si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$.

Démonstration

Étape 1 (point 1). Si $b = ka$ et $c = k'b$ avec $k, k' \in \mathbb{Z}$, alors $c = (k'k)a$ et $k'k \in \mathbb{Z}$: donc $a \mid c$.

Étape 2 (point 2). Si $b = ka$ et $c = k'a$, alors $b\lambda + c\mu = (k\lambda + k'\mu)a$ avec $k\lambda + k'\mu \in \mathbb{Z}$: donc $a \mid b\lambda + c\mu$.

Étape 3 (point 3). Si $b = ka$ et $b \neq 0$, alors $k \neq 0$, donc $|k| \geq 1$ et $|b| = |k|\,|a| \geq |a|$.

Étape 4 (point 4). Si $a = 0$, alors $b = 0$ car $a \mid b$, donc $a = b$. Si $a \neq 0$, alors $b \neq 0$ car $b \mid a$. Le point 3 donne $|a| \leq |b|$ et $|b| \leq |a|$. Donc $|a| = |b|$, c'est-à-dire $a = b$ ou $a = -b$.

À toi : Une combinaison qui élimine k

Soient k un entier relatif et n un entier relatif qui divise $5k + 3$ et $2k + 1$. Montre que $n = 1$ ou $n = -1$.

Indice 1

Cherche des entiers u et v tels que $u(5k + 3) + v(2k + 1)$ ne dépende plus de k.

Indice 2

Essaie $u = 2$ et $v = -5$: les termes en k disparaissent.

Indice 3

Un diviseur de 1 est non nul, et sa valeur absolue vaut au plus 1.

Réponse

Éliminer k. On combine les deux entiers :

$$\begin{aligned} &2(5k + 3) - 5(2k + 1) \\ &= 10k + 6 - 10k - 5 \\ &= 1. \end{aligned}$$

Diviser 1. Comme $n \mid 5k+3$ et $n \mid 2k+1$, le point 2 des propriétés de la divisibilité donne $n \mid 1$. Or $1 \neq 0$, donc $|n| \leq 1$ par le point 3.

Conclusion. Enfin $n \neq 0$, car 0 ne divise pas 1. Donc $n = 1$ ou $n = -1$.

La division euclidienne

Rappel de 1BAC : $100 = 7 \times 14 + 2$, avec un reste 2 compris entre 0 et 6. Pour un entier négatif, le reste est encore positif : $-100 = 7 \times (-15) + 5$.

Pourquoi un tel couple existe-t-il toujours, et pourquoi un seul ? Le théorème suivant répond, preuve comprise.

Théorème : Division euclidienne dans $\mathbb{Z}$

Soient a un entier relatif et b un entier naturel non nul. Il existe un unique couple (q, r) d'entiers relatifs tel que

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

L'entier q est le **quotient** et l'entier r le **reste** de la division euclidienne de a par b.

Démonstration

Existence. Étape 1. Soit $q = E\left(\frac{a}{b}\right)$ la partie entière de $\frac{a}{b}$: c'est l'entier tel que $q \leq \frac{a}{b} < q + 1$. **Étape 2.** Comme $b > 0$, on multiplie par b : $bq \leq a < bq + b$. **Étape 3.** On pose $r = a - bq$. Alors $a = bq + r$ et $0 \leq r < b$.

Unicité. Étape 4. Supposons $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$. Alors $b(q - q') = r' - r$ et $-b < r' - r < b$. Donc $b\,|q - q'| < b$, puis $|q - q'| < 1$. Comme $q - q'$ est un entier, $q = q'$, et alors $r = a - bq = r'$.

À retenir : Ce qu'il faut retenir de la preuve

Existence : le quotient est la partie entière de $\frac{a}{b}$. On encadre $\frac{a}{b}$ entre deux entiers consécutifs, puis on multiplie par b.

Unicité : deux restes possibles diffèrent de moins de b. Leur écart est pourtant un multiple de b. Il est donc nul.

Vérifie : Une multiplication d'inégalités

À l'étape 2 de l'existence, on multiplie $q \leq \frac{a}{b} < q + 1$ par b. Pourquoi les inégalités gardent-elles leur sens ?

A. Parce que $b > 0$.

Juste.
Multiplier par un nombre strictement positif conserve l'ordre. C'est là que sert l'hypothèse « b entier naturel non nul ».

B. Parce que q est un entier.

Faux.
Le fait que q soit entier sert à l'étape 1, pour définir la partie entière. Il ne dit rien du sens des inégalités.

C. Parce que $a \geq 0$.

Faux.
Le théorème vaut aussi pour a négatif, par exemple $a = -100$. Le signe de a n'intervient pas ici.

Correction
Les inégalités gardent leur sens car $b > 0$: multiplier par un réel strictement positif conserve l'ordre. Avec un multiplicateur négatif, elles s'inverseraient.

Attention : Un reste n'est jamais négatif

Écrire $-23 = 4 \times (-5) - 3$ n'est pas une division euclidienne : le reste -3 sort de l'encadrement $0 \leq r < 4$. La bonne écriture est $-23 = 4 \times (-6) + 1$.

Sans l'encadrement, l'unicité tombe : $-23 = 4 \times (-7) + 5$ est vraie aussi. Seul le reste 1 vérifie $0 \leq r < 4$.

Congruences

Le langage des congruences

Devine : L'horloge

Il est 22 h. Quelle heure affichera une horloge de 24 heures dans 100 heures ?

A. 22 h, car 100 heures font quatre jours.

Faux.
Quatre jours font 96 heures, pas 100 : il reste 4 heures à ajouter.

B. 4 h

Faux.
4 est le reste de 100 par 24. Il faut encore l'ajouter à l'heure de départ : $22 + 4 = 26$, soit 2 h.

C. 2 h

Juste.
$22 + 100 = 122 = 24 \times 5 + 2$: l'horloge affiche le reste, 2.

Indice 1

> Une horloge de 24 heures revient au même affichage toutes les 24 heures.
>
> **Correction**
> On calcule $22 + 100 = 122$, puis $122 = 24 \times 5 + 2$ avec $0 \leq 2 < 24$. L'horloge affiche 2 h : elle ne retient que le reste de la division par 24.

L'horloge calcule **modulo** 24 : deux instants séparés par un multiple de 24 heures s'affichent pareil. En 1BAC, tu as noté cette relation avec le symbole $\equiv$. Voici la définition exacte.

Définition : Congruence modulo n

Soit n un entier naturel non nul. Deux entiers relatifs a et b sont **congrus modulo** n si $n \mid a - b$. On écrit alors $a \equiv b\ [n]$, et on lit « a est congru à b modulo n ».

Exemple : Lire une congruence

- $122 \equiv 2\ [24]$, car $122 - 2 = 120 = 24 \times 5$.
- $-3 \equiv 4\ [7]$, car $-3 - 4 = -7$.

Remarque que 122 et 2 ont le même reste, 2, dans la division par 24. Est-ce un hasard ? Non : la propriété suivante l'affirme, et sa preuve compare les deux restes.

Congruence et reste

Propriété : Congruence et reste

Soient n un entier naturel non nul et a, b deux entiers relatifs.

1. $a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.
2. Tout entier relatif a est congru modulo n à son reste r, et à aucun autre entier de $\{0, 1, \ldots, n-1\}$.

Démonstration

Étape 1. On écrit $a = nq + r$ et $b = nq' + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$ (« Division euclidienne dans $\mathbb{Z}$ »). Alors $a - b = n(q - q') + (r - r')$.

Étape 2 (point 1, sens direct). Si $n \mid a - b$, alors $n \mid (a - b) - n(q - q') = r - r'$ (« Propriétés de la divisibilité »). Or $-n < r - r' < n$, car $0 \leq r < n$ et $0 \leq r' < n$: si $r - r' \neq 0$, le point 3 de « Propriétés de la divisibilité » donnerait $n \leq |r - r'|$. Donc $r = r'$.

Étape 3 (point 1, réciproque). Si $r = r'$, alors $a - b = n(q - q')$, donc $n \mid a - b$.

Étape 4 (point 2). $a - r = nq$, donc $a \equiv r\ [n]$. Si $a \equiv s\ [n]$ avec $0 \leq s \leq n-1$, le reste de s est s lui-même ($s = n \times 0 + s$) ; le point 1 donne $s = r$.

Vérifie : Un reste à trouver

Quel est le reste de la division euclidienne de -38 par 9 ?

A. 2

Faux.
C'est le reste de 38, pas de -38 : $38 = 9 \times 4 + 2$. Le signe change tout.

B. 7

Juste.
On a $-38 = 9 \times (-5) + 7$, avec $0 \leq 7 < 9$.

C. -2

Faux.
L'égalité $-38 = 9 \times (-4) - 2$ est exacte, mais un reste n'est jamais négatif. Il faut descendre d'un multiple de 9.

Indice 1
Le reste doit vérifier $0 \leq r < 9$.
Indice 2
Cherche le multiple de 9 juste en dessous de -38.

Correction
On a $-38 = 9 \times (-5) + 7$ et $0 \leq 7 < 9$: le reste est 7. Donc $-38 \equiv 7\ [9]$, et 7 est le seul entier de $\{0, 1, \ldots, 8\}$ congru à -38 modulo 9.

Calculer sans poser le produit

Cherche le reste de 47×53 dans la division par 5. Inutile de poser le produit : $47 \equiv 2\ [5]$ et $53 \equiv 3\ [5]$. On calcule $2 \times 3 = 6 \equiv 1\ [5]$.

Vérification : $47 \times 53 = 2491$, dont le reste est bien 1. Pourquoi peut-on remplacer chaque facteur par son reste ? La propriété suivante le prouve.

Propriété : Opérations sur les congruences

Soit n un entier naturel non nul.

1. Pour tous entiers relatifs a, b, c : $a \equiv a\ [n]$; si $a \equiv b\ [n]$, alors $b \equiv a\ [n]$; si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.
2. Pour tous entiers relatifs a, b, c, d : si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$.
3. Pour tous entiers relatifs a, b : si $a \equiv b\ [n]$, alors $a^k \equiv b^k\ [n]$ pour tout entier naturel k.

Démonstration

Étape 1 (point 1). $a - a = 0 = n \times 0$; $b - a = -(a - b)$; $a - c = (a - b) + (b - c)$. On conclut par le point 2 de « Propriétés de la divisibilité ».

Étape 2 (point 2). On écrit $a - b = nk$ et $c - d = nk'$ avec $k, k' \in \mathbb{Z}$. Alors $(a + c) - (b + d) = n(k + k')$ et $ac - bd = a(c - d) + d(a - b) = n(ak' + dk)$.

Étape 3 (point 3, par récurrence sur k). Initialisation : $a^0 = 1 = b^0$ (convention $x^0 = 1$ pour tout entier x, même nul). Hérédité : si $a^k \equiv b^k\ [n]$, le point 2 appliqué à cette congruence et à $a \equiv b\ [n]$ donne $a^{k+1} = a^k \times a \equiv b^k \times b = b^{k+1}\ [n]$. Conclusion : la propriété est vraie pour tout $k \in \mathbb{N}$.

Méthode : reste d'une puissance

1. **Repérer un retour à 1** : on calcule les restes de a, a^2, a^3… modulo n, jusqu'à un exposant $k \geq 1$ tel que $a^k \equiv 1\ [n]$.
2. **Diviser l'exposant par k** : $N = kq + r$, avec $0 \leq r < k$.
3. **Conclure** : $a^N = (a^k)^q \times a^r \equiv a^r\ [n]$.

Un tel exposant k n'existe pas toujours : essaie 2 modulo 4. Le petit théorème de Fermat donnera des cas où il existe à coup sûr.

Rédaction attendue. « On a $a^k \equiv 1\ [n]$. D'après les opérations sur les congruences, $(a^k)^q \equiv 1\ [n]$, donc $a^N \equiv a^r\ [n]$. » Le module s'écrit à chaque ligne.

Exemple : Exemple guidé : une grande puissance

Montrons que $3^{2026} \equiv 4\ [7]$.

k	1	2	3	4	5	6
reste de 3^k modulo 7	3	2	6	4	5	1

On a $3^6 \equiv 1\ [7]$. Or $2026 = 6 \times 337 + 4$, avec $0 \leq 4 < 6$. D'après les opérations sur les congruences :

$$\begin{aligned} 3^{2026} &= (3^6)^{337} \times 3^4 \\ &\equiv 1 \times 81 \\ &\equiv 4\ [7]. \end{aligned}$$

À toi de rédiger

> **À toi : Une divisibilité pour tout n**
>
> Montre que, pour tout entier naturel n, $13 \mid 4^{6n+1} - 4$.

Indice 1

Calcule les restes de 4^2 et de 4^3 modulo 13.

Indice 2

Tu dois trouver $4^3 \equiv -1\ [13]$, donc $4^6 \equiv 1\ [13]$.

Indice 3

Écris $4^{6n+1} = (4^6)^n \times 4$, puis conclus en écrivant le module.

Réponse

Une puissance de 4 congrue à 1. On a $4^3 = 64 = 13 \times 5 - 1$, donc $4^3 \equiv -1\ [13]$. Puis

$$\begin{aligned} 4^6 &= (4^3)^2 \\ &\equiv (-1)^2 = 1\ [13]. \end{aligned}$$

Réduire. Soit $n \in \mathbb{N}$. D'après les opérations sur les congruences, $(4^6)^n \equiv 1\ [13]$, donc

$$\begin{aligned} 4^{6n+1} &= (4^6)^n \times 4 \\ &\equiv 4\ [13]. \end{aligned}$$

Conclusion. Ainsi $4^{6n+1} - 4 \equiv 0\ [13]$: pour tout entier naturel n, $13 \mid 4^{6n+1} - 4$.

Attention : L'exposant ne se réduit pas modulo n

Pour 3^{2026} modulo 7, une erreur fréquente consiste à réduire l'exposant modulo 7 : $2026 \equiv 3\ [7]$, puis $3^3 \equiv 6\ [7]$. C'est faux : le bon reste est 4.

L'exposant se réduit selon la longueur du cycle des restes, ici 6. Il ne se réduit pas selon le module.

Nombres premiers

Reconnaître un nombre premier

Devine : Un seul est premier

Un seul de ces entiers est premier. Lequel ?

A. 91

Faux.

$91 = 7 \times 13$. Il n'est divisible ni par 2, ni par 3, ni par 5 : c'est ce qui trompe.

B. 87

Faux.

$87 = 3 \times 29$: la somme de ses chiffres, 15, est un multiple de 3.

C. 97

Juste.

Aucun des premiers 2, 3, 5 et 7 ne divise 97, et $11^2 = 121 > 97$. Tu verras pourquoi on peut s'arrêter là.

D. 51

Faux.

$51 = 3 \times 17$: la somme de ses chiffres, 6, est un multiple de 3.

Indice 1

Teste la divisibilité par 3 avec la somme des chiffres.

Indice 2

Il en reste deux : teste-les par 7.

Correction

97 est premier ; $91 = 7 \times 13$, $87 = 3 \times 29$ et $51 = 3 \times 17$ sont composés. Un entier impair qui « a l'air premier » ne l'est pas forcément : il faut tester ses diviseurs.

Définition : Nombre premier

Un entier naturel p est **premier** si $p \geq 2$ et si ses seuls diviseurs positifs sont 1 et p. On note $\mathbb{P}$ l'ensemble des nombres premiers. Un entier naturel $n \geq 2$ qui n'est pas premier est dit **composé**.

Exemple : Trois remarques

- 2 est le seul nombre premier pair : tout autre entier pair est divisible par 2.
- 1 n'est pas premier : la définition exige $p \geq 2$.
- 221 est composé, car $221 = 13 \times 17$.

Tester la primalité

Le plus petit diviseur de 91 supérieur ou égal à 2 est 7, et $7^2 = 49 \leq 91$. Pour 221, c'est 13, et $13^2 = 169 \leq 221$. Dans les deux cas, ce plus petit diviseur est premier.

Pourquoi ? Un diviseur plus petit de lui diviserait aussi l'entier de départ. La propriété suivante le prouve.

Propriété : Plus petit diviseur premier

Soit n un entier naturel, $n \geq 2$.

1. Le plus petit diviseur p de n tel que $p \geq 2$ est un nombre premier. En particulier, n admet au moins un diviseur premier.
2. Si n est composé, alors $p^2 \leq n$.
3. Par conséquent, si aucun nombre premier p tel que $p^2 \leq n$ ne divise n, alors n est premier.

Démonstration

Étape 1. L'ensemble des diviseurs k de n tels que $2 \leq k \leq n$ contient n : il est fini et non vide, il a donc un plus petit élément p.

Étape 2 (point 1). Soit c un diviseur positif de p avec $c \neq 1$. Alors $c \geq 2$ et $c \mid n$ (« Propriétés de la divisibilité », point 1). Par minimalité de p, $c \geq p$; or $c \leq p$ (« Propriétés de la divisibilité », point 3). Donc $c = p$: p est premier.

Étape 3 (point 2). Si n est composé, on écrit $n = pm$ avec m entier naturel ($n, p > 0$) ; $m \neq 1$, sinon $n = p$ serait premier. Ainsi $m \mid n$ et $2 \leq m \leq n$ (« Propriétés de la divisibilité », point 3), donc $m \geq p$ par minimalité. D'où $n = pm \geq p^2$.

Étape 4 (point 3). C'est la contraposée : si n est composé, son plus petit diviseur $p \geq 2$ est premier, divise n et vérifie $p^2 \leq n$.

Méthode **: montrer qu'un entier est premier**

1. **Borner la recherche** : on liste les nombres premiers p tels que $p^2 \leq n$.
2. **Tester chacun** : on vérifie qu'aucun ne divise n, en donnant le reste.
3. **Conclure** : si n était composé, il aurait un diviseur premier p tel que $p^2 \leq n$.

Rédaction attendue. « Les nombres premiers p tels que $p^2 \leq n$ sont … ; aucun ne divise n. D'après la propriété du plus petit diviseur premier, n est premier. »

Exemple **: Exemple guidé : 389 est-il premier ?**

On a $19^2 = 361 \leq 389 < 529 = 23^2$. On teste donc $2, 3, 5, 7, 11, 13, 17$ et 19.

p	2	3	5	7	11	13	17	19
reste de 389	1	2	4	4	4	12	15	9

Aucun reste n'est nul. D'après la propriété du plus petit diviseur premier, 389 est premier.

Une infinité de nombres premiers

Les nombres premiers se raréfient : il y en a 25 entre 1 et 100, mais seulement 14 entre 901 et 1000. Finissent-ils par s'arrêter ?

Non. Pourquoi est-ce vrai ? L'idée : multiplier tous les premiers d'une liste, ajouter 1, puis regarder un diviseur premier du résultat.

Théorème **: Infinité des nombres premiers**

L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration

Supposons par l'absurde que $\mathbb{P}$ soit fini. Il n'est pas vide, car 2 est premier (ses diviseurs positifs sont au plus 2 par « Propriétés de la divisibilité », point 3, donc ce sont 1 et 2) : on écrit $\mathbb{P} = \{p_1, p_2, \dots, p_k\}$.

Étape 1. On pose $N = p_1 p_2 \cdots p_k + 1$. Comme $p_1 p_2 \cdots p_k \geq 2$, on a $N \geq 3$. D'après « Plus petit diviseur premier », N admet un diviseur premier p.

Étape 2. Comme $\mathbb{P}$ contient tous les nombres premiers, p est l'un des p_i. Donc p divise le produit $p_1 p_2 \cdots p_k$.

Étape 3. p divise N et $p_1 p_2 \cdots p_k$, donc il divise leur différence 1 (« Propriétés de la divisibilité », point 2). Or $p \geq 2$ et le point 3 de « Propriétés de la divisibilité » donnerait $p \leq 1$: c'est une contradiction.

Conclusion. L'ensemble $\mathbb{P}$ est infini.

À retenir : Ce qu'il faut retenir de la preuve

On raisonne **par l'absurde** : on suppose la liste des nombres premiers finie.

On fabrique alors un entier N qu'aucun premier de la liste ne divise. Or N possède un diviseur premier : la liste n'était pas complète.

Vérifie : L'argument de l'étape 3

À l'étape 3, p divise N et le produit $p_1 p_2 \cdots p_k$. Quel argument conduit à la contradiction ?

A. p divise leur différence 1, alors que $p \geq 2$.

Juste.
Un diviseur commun divise la différence (propriétés de la divisibilité, point 2). Un diviseur de 1 vaut au plus 1 : impossible pour $p \geq 2$.

B. p divise N, donc N n'est pas premier.

Faux.
La preuve ne suppose jamais N premier : ce ne serait pas une contradiction. D'ailleurs p pourrait être égal à N.

C. N est premier, donc il manque à la liste.

Faux.
Rien ne dit que N est premier : l'exemple qui suit le montre avec $30031 = 59 \times 509$. La contradiction vient du diviseur premier p, pas de N.

Correction

p divise N et $p_1 p_2 \cdots p_k$, donc il divise $N - p_1 p_2 \cdots p_k = 1$. Comme $1 \neq 0$, cela donne $p \leq 1$, ce qui contredit $p \geq 2$. L'hypothèse « $\mathbb{P}$ est fini » est donc fausse.

Exemple : N n'est pas forcément premier

La preuve n'affirme pas que N est premier. Avec les six plus petits nombres premiers :

$$\begin{aligned} &2 \times 3 \times 5 \times 7 \\ &\quad \times 11 \times 13 + 1 \\ &= 30031 = 59 \times 509. \end{aligned}$$

Ce qui compte : N a un diviseur premier, et ce diviseur n'est pas dans la liste de départ.

PGCD, PPCM et algorithme d'Euclide

PGCD et PPCM

Vérifie : Le plus grand diviseur commun

Quel est le plus grand entier naturel qui divise à la fois 84 et 120 ?

A. 6

Faux.

6 divise bien 84 et 120, mais ce n'est pas le plus grand diviseur commun.

B. 840

Faux.

840 est le plus petit multiple commun non nul, pas un diviseur commun : il dépasse 84.

C. 4

Faux.

4 est un diviseur commun, mais il oublie le facteur 3, commun aux deux.

D. 12

Juste.

12 divise 84 et 120, et aucun diviseur de 84 plus grand que 12 ne divise 120.

Indice 1

Liste les diviseurs positifs de 84, puis garde ceux qui divisent 120.

Correction

Les diviseurs positifs de 84 sont 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 et 84.

Parmi eux, ceux qui divisent 120 sont 1, 2, 3, 4, 6 et 12. Le plus grand est 12.

En 1BAC, tu as noté ce nombre $a \wedge b$: c'est le **PGCD**. Le plus petit multiple commun non nul se note $a \vee b$: c'est le **PPCM**. Voici les définitions exactes.

Définition : PGCD et PPCM

Soient a et b deux entiers relatifs non tous les deux nuls. Le **plus grand commun diviseur** de a et b est le plus grand entier naturel qui divise à la fois a et b ; on le note $a \wedge b$. Si a et b sont tous les deux non nuls, le **plus petit commun multiple** de a et b est le plus petit entier naturel non nul qui est à la fois un multiple de a et un multiple de b ; on le note $a \vee b$.

Exemple : Quatre calculs

- $(-18) \wedge 30 = 6$: le signe ne change pas les diviseurs.
- $18 \vee 30 = 90$.
- $7 \wedge 0 = 7$, car tout entier divise 0.
- $8 \wedge 15 = 1$: leur seul diviseur commun positif est 1.

PGCD et reste

Cherche $391 \wedge 299$. On écrit $391 = 299 \times 1 + 92$. Un diviseur commun à 391 et 299 divise $391 - 299 = 92$. À l'inverse, un diviseur commun à 299 et 92 divise $299 + 92 = 391$.

Pourquoi est-ce utile ? On remplace le couple par un couple plus petit, sans changer le PGCD.

Propriété : PGCD et division euclidienne

Soient a un entier relatif, b un entier naturel non nul, et r le reste de la division euclidienne de a par b. Les diviseurs communs à a et b sont exactement les diviseurs communs à b et r. En particulier, $a \wedge b = b \wedge r$; si $r = 0$, alors $a \wedge b = b \wedge 0 = b$.

Démonstration

Étape 1. On écrit $a = bq + r$ (« Division euclidienne dans $\mathbb{Z}$ »). Si $c \mid a$ et $c \mid b$, alors $c \mid a - bq = r$ (« Propriétés de la divisibilité », point 2).

Étape 2. Si $c \mid b$ et $c \mid r$, alors $c \mid bq + r = a$ (« Propriétés de la divisibilité », point 2).

Étape 3. Les deux ensembles de diviseurs communs sont donc égaux ; ils ont le même plus grand élément positif : $a \wedge b = b \wedge r$. Si $r = 0$, les diviseurs communs à b et 0 sont les diviseurs de b, dont le plus grand est b : donc $b \wedge 0 = b$.

> **Vérifie : Quelle égalité en découle ?**
>
> On a $1000 = 7 \times 142 + 6$. Laquelle de ces égalités découle de la propriété précédente ?

A. $1000 \wedge 7 = 7 \wedge 6$

Juste.
On garde le diviseur 7 et on remplace 1000 par le reste 6.

B. $1000 \wedge 7 = 1000 \wedge 6$

Faux.
On garde le dividende au lieu du diviseur. D'ailleurs $1000 \wedge 6 = 2$, alors que $1000 \wedge 7 = 1$.

C. $1000 \wedge 7 = 142 \wedge 6$

Faux.
142 est le quotient : il n'intervient pas. Ici $142 \wedge 6 = 2$, alors que $1000 \wedge 7 = 1$.

Correction
Avec $a = 1000$, $b = 7$ et $r = 6$, la propriété donne $1000 \wedge 7 = 7 \wedge 6$. On recommence : $7 = 6 \times 1 + 1$, donc $7 \wedge 6 = 6 \wedge 1 = 1$.

L'algorithme d'Euclide

On peut répéter ce remplacement. Les restes diminuent strictement et restent positifs : ils finissent par s'annuler.

Pourquoi le dernier reste non nul est-il le PGCD ? Chaque division conserve le PGCD, jusqu'au dernier couple $(r_m, 0)$, et $r_m \wedge 0 = r_m$.

Propriété : Algorithme d'Euclide

Soient a et b deux entiers naturels non nuls. On pose $r_0 = a$ et $r_1 = b$, puis, tant que $r_k \neq 0$, on note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k. Il existe un rang $m \geq 1$ tel que $r_m \neq 0$ et $r_{m+1} = 0$, et alors

$$a \wedge b = r_m.$$

Le PGCD de a et b est le dernier reste non nul.

Démonstration

Étape 1 (l'algorithme s'arrête). Tant que les restes sont non nuls, on a $b = r_1 > r_2 > r_3 > \cdots \geq 0$, car chaque reste est strictement inférieur au diviseur (« Division euclidienne dans $\mathbb{Z}$ »). Une suite strictement décroissante d'entiers naturels ne peut pas avoir plus de $b + 1$ termes : un reste finit par être nul.

Étape 2. Soit m le rang tel que $r_m \neq 0$ et $r_{m+1} = 0$. Par « PGCD et division euclidienne » appliqué à chaque division, $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$ pour $1 \leq k \leq m$.

Étape 3. De proche en proche (récurrence sur k), $a \wedge b = r_0 \wedge r_1 = r_m \wedge r_{m+1} = r_m \wedge 0 = r_m$.

Méthode : l'algorithme d'Euclide en tableau

1. **Ranger** : on divise le plus grand entier par le plus petit, sur une ligne du tableau.
2. **Décaler** : le diviseur devient le dividende, le reste devient le diviseur.
3. **S'arrêter** au premier reste nul, et lire le reste de la ligne précédente.

Rédaction attendue. « D'après l'algorithme d'Euclide, $a \wedge b$ est le dernier reste non nul. » Chaque ligne respecte l'encadrement du reste.

Exemple : Exemple guidé : 391 et 299

dividende	diviseur	quotient	reste
391	299	1	92
299	92	3	23
92	23	4	0

Le dernier reste non nul est 23. D'après l'algorithme d'Euclide, $391 \wedge 299 = 23$. Garde ce tableau : il resservira dans la section suivante.

Premiers entre eux et théorème de Bézout

Ce que donnent les combinaisons

Prouver que deux expressions en n sont premières entre elles tient en deux lignes, à condition de savoir fabriquer un 1.

Ce 1 s'écrit avec les deux nombres : c'est toute l'idée de Bézout. Commence par une petite enquête.

> **Devine : Des combinaisons de 6 et 10**
>
> On cherche des entiers relatifs u et v tels que $6u + 10v$ vaille 1, puis 2. Qu'en penses-tu ?
>
> **A.** On peut obtenir 1 et 2.
> **Faux.**
> $6u + 10v = 2(3u + 5v)$ est toujours pair : il ne vaut jamais 1.
>
> **B.** On ne peut pas obtenir 1, mais on peut obtenir 2.
> **Juste.**
> $6u + 10v$ est pair, donc différent de 1. Et $6 \times 2 + 10 \times (-1) = 2$.
>
> **C.** On peut obtenir 1, mais pas 2.
> **Faux.**
> Tout est pair dans $6u + 10v$: si 1 était atteint, il serait pair.

D. On n'obtient ni 1 ni 2.

Faux.

2 est atteint : $6 \times 2 + 10 \times (-1) = 12 - 10 = 2$.

Indice 1

Factorise $6u + 10v$ par 2.

Indice 2

Pour obtenir 2, essaie $u = 2$.

Correction

$6u + 10v = 2(3u + 5v)$ est toujours pair : 1 est impossible. Le couple $(2, -1)$ donne $6 \times 2 + 10 \times (-1) = 2$. Le plus petit entier strictement positif atteint est donc 2, c'est-à-dire $6 \wedge 10$.

Définition : Entiers premiers entre eux

Deux entiers relatifs a et b, non tous les deux nuls, sont **premiers entre eux** si $a \wedge b = 1$, c'est-à-dire si leur seul diviseur commun positif est 1.

Exemple : Premiers entre eux ou non ?

- $9 \wedge 28 = 1$: 9 et 28 sont premiers entre eux, sans être premiers.
- $21 \wedge 35 = 7$: ils ne sont pas premiers entre eux.

L'identité de Bézout

Pourquoi le PGCD est-il toujours une combinaison $au + bv$? Idée : on prend la plus petite combinaison strictement positive, et on montre qu'elle divise a et b.

Rappel. Toute partie non vide de $\mathbb{N}$ possède un plus petit élément. Par exemple, les entiers naturels non nuls de la forme $6u + 10v$ ont pour plus petit élément 2.

Théorème : Identité de Bézout

Soient a et b deux entiers relatifs non tous les deux nuls, et $d = a \wedge b$.

1. Il existe deux entiers relatifs u et v tels que $au + bv = d$.
2. Un entier relatif divise à la fois a et b si et seulement s'il divise d.

Démonstration

Étape 1. L'ensemble E des entiers naturels non nuls de la forme $au + bv$, avec $u, v \in \mathbb{Z}$, contient $a^2 + b^2 = a \times a + b \times b > 0$. Partie non vide de $\mathbb{N}$, il a donc un plus petit élément $m = au_0 + bv_0$.

Étape 2 ($m \mid a$). On écrit $a = mq + r$ avec $0 \leq r < m$ (« Division euclidienne dans $\mathbb{Z}$ »). Alors $r = a(1 - qu_0) + b(-qv_0)$. Si $r > 0$, alors $r \in E$ et $r < m$: impossible. Donc $r = 0$ et $m \mid a$. De même, $m \mid b$.

Étape 3 ($m = d$). m est un diviseur commun positif, donc $m \leq d$. Or $d \mid a$ et $d \mid b$, donc $d \mid au_0 + bv_0 = m$ (« Propriétés de la divisibilité », point 2), puis $d \leq m$ (« Propriétés de la divisibilité », point 3). Ainsi $d = m = au_0 + bv_0$.

Étape 4 (point 2). Si $c \mid a$ et $c \mid b$, alors $c \mid au_0 + bv_0 = d$. Si $c \mid d$, alors $c \mid a$ et $c \mid b$ par transitivité (« Propriétés de la divisibilité », point 1).

À retenir : Ce qu'il faut retenir de la preuve

On ne calcule pas u et v : on prend la **plus petite** valeur strictement positive m de $au + bv$.

La division euclidienne par m et la minimalité montrent que m divise a et b. Deux inégalités, $m \leq d$ et $d \leq m$, donnent ensuite $m = d$.

Vérifie : Une inégalité de l'étape 3

À l'étape 3, comment obtient-on $d \leq m$?

A. m est le plus petit élément de E.

Faux.
La minimalité de m sert à l'étape 2. Elle compare m aux éléments de E, pas à d.

B. d est le plus grand diviseur commun et m en est un.

Faux.
Cet argument est correct, mais il donne l'autre inégalité : $m \leq d$.

C. d divise a et b, donc d divise $au_0 + bv_0 = m$, avec $m > 0$.

Juste.
Un diviseur commun divise toute combinaison, et un diviseur d'un entier non nul ne le dépasse pas (propriétés de la divisibilité, points 2 et 3).

Correction
Comme $d \mid a$ et $d \mid b$, on a $d \mid au_0 + bv_0 = m$. Or $m \neq 0$, donc $d \leq |m| = m$. Avec $m \leq d$, on obtient $d = m$.

Exemple : Ni unicité, ni cas nul

- Le couple n'est pas unique : $6 \times 2 + 10 \times (-1) = 2$ et $6 \times (-3) + 10 \times 2 = 2$.
- L'hypothèse « non tous les deux nuls » est nécessaire : si $a = b = 0$, toute combinaison vaut 0, et $a \wedge b$ n'est pas défini.

Pour $d = 1$, l'identité donne $au + bv = 1$. Et la réciproque ? Pourquoi une telle égalité suffit-elle à prouver $a \wedge b = 1$? Regarde ce que divise un diviseur commun.

Le théorème de Bézout

Théorème : Théorème de Bézout

Deux entiers relatifs a et b sont premiers entre eux si et seulement s'il existe deux entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration

Sens direct. Si $a \wedge b = 1$, alors a et b ne sont pas tous les deux nuls et l'identité de Bézout (point 1) fournit u et v tels que $au + bv = 1$.

Réciproque. Supposons $au + bv = 1$. Alors a et b ne sont pas tous les deux nuls. Soit c un diviseur commun positif de a et b. D'après « Propriétés de la divisibilité » (point 2), $c \mid au + bv = 1$, donc $c \leq 1$ (« Propriétés de la divisibilité », point 3), c'est-à-dire $c = 1$. Le seul diviseur commun positif est 1 : $a \wedge b = 1$.

À retenir : Ce qu'il faut retenir de la preuve

Le sens direct est le cas $d = 1$ de l'identité de Bézout.

La réciproque n'utilise que les propriétés de la divisibilité. Retiens surtout le rôle du 1 : son seul diviseur positif est 1.

Vérifie : La réciproque

Dans la réciproque, on suppose $au + bv = 1$. Quel argument fait passer de « c divise a et b » à « c divise 1 » ?

A. Un diviseur commun de a et b divise toute combinaison $au + bv$.

Juste.
C'est le point 2 des propriétés de la divisibilité, appliqué à $au + bv = 1$.

B. Le théorème de Gauss.

Faux.
Gauss se démontre à partir de Bézout : l'utiliser ici rendrait le raisonnement circulaire.

C. La transitivité : $c \mid a$ et $a \mid 1$.

Faux.
Rien n'assure que a divise 1 : la transitivité ne s'applique pas ici.

Correction
Si $c \mid a$ et $c \mid b$, alors $c \mid au + bv$ (propriétés de la divisibilité, point 2), c'est-à-dire $c \mid 1$. Pour c positif, cela donne $c = 1$: le seul diviseur commun positif est 1, et $a \wedge b = 1$.

Attention : La réciproque de Bézout ne vaut que pour 1

$10 \times 2 + 4 \times (-3) = 8$, et pourtant $10 \wedge 4 = 2$, pas 8.

Une égalité $au + bv = k$ montre seulement que $a \wedge b$ divise k. Pour $k = 1$, elle suffit : $a \wedge b = 1$. Pour conclure $a \wedge b = k$ avec $k \geq 2$, il faut en plus vérifier que k divise a et b.

Construire un couple de Bézout

Méthode : remonter l'algorithme d'Euclide

1. **Isoler les restes** des divisions de l'algorithme d'Euclide.
2. **Remonter** du dernier reste non nul, en remplaçant chaque reste par son expression.
3. **Vérifier** le couple trouvé par un calcul direct.

Avec le tableau de 391 et 299 : $23 = 299 - 3 \times 92$ et $92 = 391 - 299$.

$$\begin{aligned} 23 &= 299 - 3 \times (391 - 299) \\ &= 4 \times 299 - 3 \times 391. \end{aligned}$$

Rédaction attendue. « On a $391 \times (-3) + 299 \times 4 = 23 = 391 \wedge 299$: le couple $(u, v) = (-3, 4)$ convient. »

À toi : une remontée en trois étapes

L'algorithme d'Euclide donne, pour 83 et 19 : $83 = 19 \times 4 + 7$, $19 = 7 \times 2 + 5$, $7 = 5 \times 1 + 2$ et $5 = 2 \times 2 + 1$.

La remontée est commencée :

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (7 - 5) \\ &= 3 \times 5 - 2 \times 7. \end{aligned}$$

Termine-la : trouve des entiers u et v tels que $83u + 19v = 1$, puis vérifie ton couple.

Indice 1
Isole le reste 5 dans la deuxième division : $5 = 19 - 2 \times 7$.
Indice 2
Remplace 5 dans $3 \times 5 - 2 \times 7$, puis regroupe les 7 : tu dois obtenir $3 \times 19 - 8 \times 7$.
Indice 3

Garde 19 et 7 comme des briques, sans calculer les produits. Remplace enfin 7 par $83 - 4 \times 19$.

Réponse

Remonter. On remplace 5 par $19 - 2 \times 7$, puis 7 par $83 - 4 \times 19$:

$$\begin{aligned} 1 &= 3 \times 5 - 2 \times 7 \\ &= 3 \times (19 - 2 \times 7) \\ &\quad - 2 \times 7 \\ &= 3 \times 19 - 8 \times 7 \\ &= 3 \times 19 \\ &\quad - 8 \times (83 - 4 \times 19) \\ &= 35 \times 19 - 8 \times 83. \end{aligned}$$

Vérification. $83 \times (-8) + 19 \times 35 = -664 + 665 = 1$.

Conclusion. Le couple $(u, v) = (-8, 35)$ convient. D'après le théorème de Bézout, 83 et 19 sont premiers entre eux.

À toi : Coin examen

Soit n un entier naturel. Montrer que $5n + 2$ et $3n + 1$ sont premiers entre eux. *(0,5 point, barème indicatif BURHAN.)*

Point important : établir une relation $au + bv = 1$ est une question à maîtriser.

Indice 1

Cherche des entiers u et v, indépendants de n, qui éliminent n.

Indice 2

Essaie $u = 3$ et $v = -5$.

Indice 3

Conclus en citant le théorème de Bézout et le couple trouvé.

Réponse

Rédaction attendue.

On calcule une combinaison qui élimine n :

$$\begin{aligned} &3(5n + 2) - 5(3n + 1) \\ &= 15n + 6 - 15n - 5 \\ &= 1. \end{aligned}$$

(0,25 point)

Ainsi $(5n + 2) \times 3 + (3n + 1) \times (-5) = 1$, avec 3 et -5 entiers. D'après le théorème de Bézout, $5n + 2$ et $3n + 1$ sont premiers entre eux. *(0,25 point)*

Théorème de Gauss

Diviser un produit

Bézout fabrique un 1 ; Gauss s'en sert. Avec lui, tu sauras « simplifier » une divisibilité.

C'est l'outil des équations $ax + by = c$ et de la preuve du petit théorème de Fermat. Commence par une prédiction.

Devine : Deux diviseurs d'un même produit

Soit k un entier. On sait que $9 \mid 10k$ et que $15 \mid 10k$. Quelle conclusion est sûre ?

A. $9 \mid k$ et $15 \mid k$

Faux.
Avec $k = 9$: $10k = 90$ est divisible par 9 et par 15, mais $15 \nmid 9$.

B. Seule la conclusion $9 \mid k$ est sûre

Juste.
9 et 10 n'ont que 1 comme diviseur commun positif : tout le facteur 9 passe dans k. Pour 15, le facteur 5 peut venir de 10.

C. Seule la conclusion $15 \mid k$ est sûre

Faux.
C'est l'inverse : 15 partage le facteur 5 avec 10. Il peut diviser $10k$ sans diviser k, comme pour $k = 9$.

D. Aucune des deux

Faux.
$9 \mid k$ est sûr, car $9 \wedge 10 = 1$. Le théorème de cette section le prouve.

Indice 1
Compare $9 \wedge 10$ et $15 \wedge 10$.
Indice 2
Pour réfuter une conclusion, cherche un k qui vérifie les deux hypothèses.

Correction
Seule $9 \mid k$ est sûre. Comme $9 \wedge 10 = 1$, le facteur 10 n'apporte aucun diviseur de 9. En revanche, $15 \wedge 10 = 5$: avec $k = 9$, on a $15 \mid 90$ mais $15 \nmid 9$.

Ta prédiction se tranche par un théorème qui porte un nom : le **théorème de Gauss**.

Pourquoi est-il vrai ? L'outil est le théorème de Bézout, établi juste avant. La preuve, sous l'énoncé, tient en trois étapes.

Le théorème de Gauss

Théorème : Théorème de Gauss

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

Démonstration

Étape 1. Comme $a \wedge b = 1$, le théorème de Bézout donne deux entiers relatifs u et v tels que $au + bv = 1$.

Étape 2. On multiplie par c : $acu + bcv = c$.

Étape 3. a divise acu, et a divise bc par hypothèse, donc a divise bcv (« Propriétés de la divisibilité », point 1, car $bc \mid bcv$). Par « Propriétés de la divisibilité » (point 2), a divise $acu + bcv = c$.

À retenir : Ce qu'il faut retenir de la preuve

On **multiplie par** c une relation de Bézout $au + bv = 1$.

L'information sur le produit bc devient alors une information sur c lui-même. Ce geste resservira souvent : Bézout prépare, Gauss conclut.

Vérifie : Quelle hypothèse sert où ?

Dans la preuve, à quelle étape sert l'hypothèse $a \mid bc$?

A. À l'étape 1, pour obtenir u et v.

Faux.

L'étape 1 utilise $a \wedge b = 1$, à travers le théorème de Bézout.

B. Elle ne sert pas : $a \wedge b = 1$ suffit.

Faux.

Sans $a \mid bc$, rien ne relie a à c : $3 \wedge 5 = 1$, et pourtant $3 \nmid 7$.

C. À l'étape 3, pour affirmer que a divise bcv.

Juste.

Comme $a \mid bc$, a divise tout multiple de bc, en particulier bcv.

Correction

L'hypothèse $a \mid bc$ sert à l'étape 3 : elle donne $a \mid bcv$. L'hypothèse $a \wedge b = 1$ sert à l'étape 1, par Bézout. Les deux sont nécessaires.

Attention : Pas de Gauss sans primalité relative

$10 \mid 4 \times 15$, car $60 = 10 \times 6$. Pourtant $10 \nmid 4$ et $10 \nmid 15$. Ici $10 \wedge 4 = 2$: l'hypothèse $a \wedge b = 1$ manque.

Avant d'écrire « d'après le théorème de Gauss », prouve toujours la primalité relative.

Les conséquences du théorème

Avec un nombre premier, Gauss devient très maniable : si $7 \mid ab$, alors 7 divise a ou b. Avec 10, c'est faux, comme le montre $10 \mid 4 \times 15$.

De même, $4 \mid 72$ et $9 \mid 72$ donnent $36 \mid 72$, car $4 \wedge 9 = 1$. Mais $4 \mid 12$ et $6 \mid 12$, sans que 24 divise 12. Pourquoi ? Tout repose sur Gauss et la primalité relative.

Propriété : Conséquences du théorème de Gauss

Soient p un nombre premier et a, b, n des entiers relatifs.

1. Si $p \nmid a$, alors $a \wedge p = 1$.
2. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.
3. Si $a \mid n$, $b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$.
4. Si p divise un produit $a_1 a_2 \cdots a_s$ d'entiers relatifs ($s \geq 1$), alors p divise l'un des a_i.

Démonstration

Étape 1 (point 1). Soit c un diviseur commun positif de a et p. Comme $c \mid p$ et p est premier, $c = 1$ ou $c = p$. Or $p \nmid a$, donc $c \neq p$. Ainsi $c = 1$ et $a \wedge p = 1$.

Étape 2 (point 2). Si $p \mid a$, c'est terminé. Sinon, $a \wedge p = 1$ d'après le point 1. Comme $p \mid ab$, le théorème de Gauss donne $p \mid b$.

Étape 3 (point 3). On écrit $n = ak$ avec $k \in \mathbb{Z}$. Alors $b \mid ak$ et $b \wedge a = 1$, donc $b \mid k$ (« Théorème de Gauss »). On écrit $k = bk'$: $n = abk'$, donc $ab \mid n$.

Étape 4 (point 4, par récurrence sur s). Pour $s = 1$, l'hypothèse est la conclusion. Si le résultat vaut pour s facteurs et si $p \mid (a_1 \cdots a_s)\, a_{s+1}$, le point 2 donne $p \mid a_1 \cdots a_s$ ou $p \mid a_{s+1}$; dans le premier cas, p divise l'un des a_i par hypothèse de récurrence.

Vérifie : Deux diviseurs de n

On sait que $8 \mid n$ et $15 \mid n$. Quelle conclusion est justifiée ?

A. $120 \mid n$, car $8 \wedge 15 = 1$.
Juste.
C'est le point 3 : 8 et 15 divisent n et sont premiers entre eux, donc $8 \times 15 = 120$ divise n.

B. $23 \mid n$, car $8 + 15 = 23$.
Faux.
Les diviseurs ne s'additionnent pas : $n = 120$ vérifie les hypothèses, et $23 \nmid 120$.

C. On ne peut rien conclure de plus.
Faux.
Comme $8 \wedge 15 = 1$, le point 3 s'applique et donne $120 \mid n$.

Correction
On a $8 \mid n$, $15 \mid n$ et $8 \wedge 15 = 1$. D'après le point 3 des conséquences du théorème de Gauss, $8 \times 15 = 120$ divise n.

Appliquer Gauss

Méthode : appliquer le théorème de Gauss

1. **Repérer le produit** : on obtient une relation du type $a \mid bc$.
2. **Établir** $a \wedge b = 1$: par une relation de Bézout, ou bien parce que a est un nombre premier qui ne divise pas b.
3. **Conclure en citant** le théorème et ses deux hypothèses.

Rédaction attendue. « On a $a \mid bc$ et $a \wedge b = 1$. D'après le théorème de Gauss, $a \mid c$. »

Exemple : Exemple guidé : une égalité de produits

Soient x et y des entiers tels que $11x = 7y$. Montrons que $7 \mid x$.

On a $7 \mid 7y$, donc $7 \mid 11x$. Or 7 est premier et $7 \nmid 11$, donc $7 \wedge 11 = 1$. D'après le théorème de Gauss, $7 \mid x$.

On écrit alors $x = 7k$ avec $k \in \mathbb{Z}$. L'égalité $11 \times 7k = 7y$ donne $y = 11k$.

À toi : Coin examen

Soient p un nombre premier tel que $p \geq 5$, et a un entier tel que $p \mid 12a$. Montrer que $p \mid a$. *(1 point, barème indicatif BURHAN.)*

Indice 1
Montre d'abord que $p \nmid 12$: quels sont les diviseurs positifs de 12 ?
Indice 2
Un nombre premier qui ne divise pas 12 est premier avec 12.
Indice 3
Nomme le théorème de Gauss et ses deux hypothèses.

Réponse
Rédaction attendue.

Les diviseurs positifs de 12 sont $1, 2, 3, 4, 6$ et 12. Aucun n'est un nombre premier supérieur ou égal à 5, donc $p \nmid 12$. *(0,25 point)*

Comme p est premier et $p \nmid 12$, on a $p \wedge 12 = 1$ (conséquences du théorème de Gauss, point 1). *(0,25 point)*

> On a $p \mid 12a$ et $p \wedge 12 = 1$. D'après le théorème de Gauss, $p \mid a$. *(0,5 point)*

Décomposition en facteurs premiers

Retrouver la décomposition

> **Vérifie : La décomposition de 360**
>
> Tu as appris en 1BAC à décomposer un entier en produit de facteurs premiers. Laquelle de ces écritures est la décomposition de 360 ?
>
> **A.** $2^3 \times 45$
>
> **Faux.**
> Le produit vaut bien 360, mais $45 = 3^2 \times 5$ n'est pas premier : la décomposition n'est pas finie.
>
> **B.** $4 \times 9 \times 10$
>
> **Faux.**
> Le produit vaut 360, mais aucun de ces trois facteurs n'est premier.
>
> **C.** $2^3 \times 3^2 \times 5$
>
> **Juste.**
> Chaque facteur est premier, et le produit vaut $8 \times 9 \times 5 = 360$.
>
> **D.** $2^2 \times 3^2 \times 5$
>
> **Faux.**
> Ce produit vaut 180 : un facteur 2 s'est perdu en route.
>
> **Indice 1**
> Un nombre premier n'a que deux diviseurs positifs : 1 et lui-même.
> **Indice 2**
> Divise 360 par 2 autant de fois que possible, puis par 3, puis par 5.
>
> **Correction**
> On divise par 2 tant que c'est possible, puis par 3 :
>
> $$\begin{aligned} 360 &= 2 \times 180 = 2^2 \times 90 \\ &= 2^3 \times 45 \\ &= 2^3 \times 3^2 \times 5. \end{aligned}$$
>
> Seule l'écriture $2^3 \times 3^2 \times 5$ ne contient que des nombres premiers et vaut 360.

Rappel de 1BAC. On divise par le plus petit nombre premier possible, puis on recommence avec le quotient, comme pour 360. Le théorème suivant dit que cette écriture existe toujours, et qu'elle est **unique**. Sous l'énoncé, tu lis une idée de la preuve : les grandes étapes, pas tous les détails.

> Théorème **: Théorème fondamental de l'arithmétique**

Tout entier naturel $n \geq 2$ s'écrit comme un produit de nombres premiers, et cette écriture est unique à l'ordre des facteurs près. En regroupant les facteurs égaux :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

où l'entier k, les nombres premiers $p_1 < p_2 < \cdots < p_k$ et les entiers naturels non nuls $\alpha_1, \ldots, \alpha_k$ sont uniques.

Démonstration

Idée de la preuve.

Existence. Supposons par l'absurde qu'il existe des entiers $n \geq 2$ sans écriture en produit de nombres premiers, et soit n le plus petit d'entre eux. Un nombre premier est un produit à un seul facteur : n n'est donc pas premier, et $n = pm$, où p est son plus petit diviseur premier (« Plus petit diviseur premier ») et $2 \leq m < n$ (car $p \geq 2$ et n composé). Par minimalité de n, m est un produit de nombres premiers, donc $n = pm$ aussi : contradiction.

Unicité. Si un nombre premier p divise un produit de nombres premiers $p'_1 p'_2 \cdots p'_s$, le point 4 de « Conséquences du théorème de Gauss » montre que p divise l'un des p'_j, donc $p = p'_j$. Dans deux écritures du même entier, on simplifie ainsi les facteurs un à un.

Étape omise : la récurrence sur le nombre de facteurs.

Exemple : L'unicité au travail

Existe-t-il des entiers $m \geq 1$ et $k \geq 1$ tels que $10^m = 6^k$?

On décompose : $10^m = 2^m \times 5^m$ et $6^k = 2^k \times 3^k$. Le facteur premier 5 figure dans la première écriture, pas dans la seconde. Par unicité de la décomposition, ces deux entiers ne sont jamais égaux. La réponse est donc non.

Diviseurs, PGCD et PPCM

Un diviseur positif de $1980 = 2^2 \times 3^2 \times 5 \times 11$ se fabrique en choisissant les exposants : 0, 1 ou 2 pour le facteur 2, de même pour 3, puis 0 ou 1 pour 5 et pour 11. Par exemple, $2 \times 3^2 \times 11 = 198$ divise 1980. L'énoncé suivant généralise cette idée. Sa preuve est, elle aussi, une idée de la preuve.

Propriété : Diviseurs, PGCD et PPCM par la décomposition

Soient $p_1 < p_2 < \cdots < p_k$ des nombres premiers.

1. Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ avec des exposants α_i entiers naturels, les diviseurs positifs de n sont les entiers $p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ avec $0 \leq \gamma_i \leq \alpha_i$ pour tout i. Leur nombre est $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

2. Si $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ et $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, avec des exposants entiers naturels éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)} \quad \text{et} \quad a \vee b = p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}.$$

3. Pour tous entiers naturels non nuls a et b : $(a \wedge b)(a \vee b) = ab$.

Démonstration

Idée de la preuve.

Point 1. Un premier qui divise un diviseur positif c de n divise n : c'est l'un des p_i (« Conséquences du théorème de Gauss », point 4). Par l'unicité (« Théorème fondamental de l'arithmétique »), l'exposant de p_i dans c ne dépasse pas α_i : $\alpha_i + 1$ choix pour γ_i.

Point 2. Par le point 1, un diviseur positif commun a des exposants $\gamma_i \leq \min(\alpha_i, \beta_i)$: il divise $p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)}$, qui est donc le plus grand. Un multiple commun non nul a, en chaque p_i, un exposant au moins égal à $\max(\alpha_i, \beta_i)$: il est multiple de $p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)}$, qui est donc le plus petit.

Point 3. On écrit a et b sur la même liste de premiers ; pour tout i, $\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i$.

Étapes omises : la comparaison des exposants par l'unicité (« Théorème fondamental de l'arithmétique ») ; deux choix d'exposants distincts donnent deux diviseurs distincts.

Exemple : 1980 et 1650

On a $1980 = 2^2 \times 3^2 \times 5 \times 11$ et $1650 = 2 \times 3 \times 5^2 \times 11$.

- **Nombre de diviseurs** de 1980 : $(2+1)(2+1)(1+1)(1+1) = 36$.
- **PGCD** : on garde les plus petits exposants, $1980 \wedge 1650 = 2 \times 3 \times 5 \times 11 = 330$.
- **PPCM** : on garde les plus grands exposants, $1980 \vee 1650 = 2^2 \times 3^2 \times 5^2 \times 11 = 9900$.
- **Contrôle** : $330 \times 9900 = 3\,267\,000 = 1980 \times 1650$.

Attention : Compter les diviseurs

On a $180 = 2^2 \times 3^2 \times 5$. Son nombre de diviseurs positifs est $(2+1)(2+1)(1+1) = 18$, et non $2 \times 2 \times 1 = 4$. Chaque exposant peut aussi valoir 0 : c'est le « $+1$ » de chaque facteur.

À toi : Un PGCD sans Euclide

Soient $a = 2^3 \times 3 \times 5^2$ et $b = 2 \times 3^4 \times 11$. Que vaut $a \wedge b$?

A. $2^3 \times 3^4 \times 5^2 \times 11$

Faux.

C'est le PPCM : tu as gardé les plus grands exposants.

B. $2 \times 3 = 6$

Juste.

Les facteurs communs sont 2 et 3 ; on garde les plus petits exposants, 1 et 1.

C. $2^4 \times 3^5$

Faux.

Tu as additionné les exposants des facteurs communs : c'est ce qu'on fait pour un produit, pas pour le PGCD.

D. 1

Faux.

a et b sont tous deux pairs : 2 est un diviseur commun, donc $a \wedge b \geq 2$.

Indice 1

Repère les facteurs premiers présents dans les deux décompositions.

Indice 2

Pour chacun, garde le plus petit des deux exposants.

Correction

Les facteurs premiers communs sont 2 (exposants 3 et 1) et 3 (exposants 1 et 4). Les facteurs 5 et 11 ne figurent que dans une décomposition : leur plus petit exposant est 0. Donc $a \wedge b = 2^1 \times 3^1 = 6$ (diviseurs, PGCD et PPCM par la décomposition, point 2).

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

Ranger les entiers par restes

Devine : Les jours de la semaine

Aujourd'hui est un mercredi. Quel jour de la semaine serons-nous dans 100 jours ?

A. Mercredi

Faux.

Ce serait vrai si 100 était un multiple de 7. Or $7 \times 14 = 98$: il reste 2 jours.

B. Vendredi

Juste.

$100 = 7 \times 14 + 2$: quatorze semaines entières, puis 2 jours après mercredi.

C. Jeudi

Faux.

Tu as compté un seul jour de reste. Or $100 - 98 = 2$: il en reste deux.

Indice 1

Le calendrier revient au même jour toutes les 7 journées.

Indice 2

Cherche le reste de 100 dans la division par 7.

Correction

$100 = 7 \times 14 + 2$, avec $0 \leq 2 < 7$: dans 100 jours, on sera 2 jours après mercredi, un vendredi. Le calendrier ne distingue pas 2, 9, 16 ou 100 jours, qui ont le même reste modulo 7. Regrouper ces entiers, c'est former une **classe**.

Définition : Classes modulo n et ensemble $\mathbb{Z}$/n$\mathbb{Z}$

Soit n un entier naturel, $n \geq 2$. Pour tout entier relatif a, la **classe** de a modulo n est l'ensemble des entiers relatifs congrus à a modulo n :

$$\overline{a} = \{\, b \in \mathbb{Z} \;/\; b \equiv a \;[n] \,\}.$$

L'ensemble des classes modulo n se note $\mathbb{Z}/n\mathbb{Z}$.

Exemple : Les classes modulo 5

Modulo 5, il y a cinq restes possibles, donc cinq tiroirs. Par exemple :

$$\overline{3} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}.$$

Ainsi $\overline{3} = \overline{8} = \overline{-2}$: n'importe quel élément peut nommer la classe. **Pourquoi** y a-t-il exactement cinq classes ? Parce que tout entier a un unique reste entre 0 et 4 : c'est l'énoncé suivant.

Combien de classes

Propriété : Description de $\mathbb{Z}$/n$\mathbb{Z}$

Soit n un entier naturel, $n \geq 2$.

1. Pour tous entiers relatifs a et b : $\overline{a} = \overline{b}$ si et seulement si $a \equiv b \;[n]$.
2. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, et ces n classes sont deux à deux distinctes.

Démonstration

Étape 1 (point 1). Si $\overline{a} = \overline{b}$, alors $a \in \overline{a}$ (car $a \equiv a \;[n]$, « Opérations sur les congruences »), donc $a \in \overline{b}$, c'est-à-dire $a \equiv b \;[n]$. Réciproquement, si $a \equiv b \;[n]$, alors pour tout entier c : $c \equiv a \;[n]$ équivaut à $c \equiv b \;[n]$ (transitivité et symétrie, « Opérations sur les congruences »). Donc $\overline{a} = \overline{b}$.

Étape 2 (point 2). Tout entier a est congru à son reste $r \in \{0, \dots, n-1\}$ (« Congruence et reste », point 2), donc $\overline{a} = \overline{r}$. Si $0 \leq r < s \leq n-1$, alors $0 < s - r < n$, donc $n \nmid s - r$ (« Propriétés de la divisibilité », point 3), soit $r \not\equiv s \ [n]$, et $\overline{r} \neq \overline{s}$ d'après le point 1.

Vérifie : Le bon représentant

Dans $\mathbb{Z}/9\mathbb{Z}$, laquelle de ces classes est égale à $\overline{40}$?

A. $\overline{5}$

Faux.
$40 - 5 = 35$ n'est pas un multiple de 9. Erreur de signe : c'est $40 + 5 = 45$ qui est un multiple de 9.

B. $\overline{36}$

Faux.
36 est le multiple de 9 le plus proche, pas un entier congru à 40 : $\overline{36} = \overline{0}$, alors que $\overline{40} = \overline{4}$.

C. $\overline{-5}$

Juste.
$40 - (-5) = 45 = 9 \times 5$, donc $40 \equiv -5 \ [9]$.

Indice 1
Dans $\mathbb{Z}/9\mathbb{Z}$, $\overline{a} = \overline{b}$ si et seulement si 9 divise $a - b$ (description de $\mathbb{Z}/n\mathbb{Z}$).
Indice 2
Calcule la différence entre 40 et chaque représentant proposé.

Correction
$40 = 9 \times 4 + 4$, donc $\overline{40} = \overline{4}$. Or $-5 = 4 - 9$, donc $\overline{-5} = \overline{4} = \overline{40}$ (description de $\mathbb{Z}/n\mathbb{Z}$, point 1). On calcule ensuite avec n'importe quel représentant : le résultat ne dépend pas de ce choix, comme le dit l'énoncé suivant.

Calculer avec des classes

Propriété : Opérations dans $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier naturel, $n \geq 2$. On définit, pour tous entiers relatifs a et b :

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \times \overline{b} = \overline{ab}.$$

Ces opérations ne dépendent pas des entiers choisis pour représenter les classes. Elles sont commutatives et associatives, la multiplication est distributive par rapport à l'addition, $\overline{0}$ est neutre pour l'addition, $\overline{1}$ est neutre pour la multiplication, et toute classe $\overline{a}$ a pour opposée $\overline{-a}$.

Démonstration

Étape 1 (les opérations sont bien définies). Si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, alors $a \equiv a'\ [n]$ et $b \equiv b'\ [n]$ (« Description de $\mathbb{Z}/n\mathbb{Z}$ »). D'après « Opérations sur les congruences », $a + b \equiv a' + b'\ [n]$ et $ab \equiv a'b'\ [n]$, donc $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$.

Étape 2 (les propriétés). Soient a, b, c des entiers relatifs. Chaque propriété se déduit de la même propriété dans $\mathbb{Z}$. Par exemple, $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$, et $\overline{a} \times (\overline{b} + \overline{c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{a} \times \overline{b} + \overline{a} \times \overline{c}$. De même, $\overline{a} + \overline{-a} = \overline{0}$. Les associativités, la commutativité de $\times$ et les neutres $\overline{0}, \overline{1}$ s'obtiennent de la même façon : on écrit chaque classe avec un représentant et on applique la propriété de $\mathbb{Z}$.

Exemple : La table de multiplication de $\mathbb{Z}/8\mathbb{Z}$

Un calcul : $\overline{5} \times \overline{6} = \overline{30} = \overline{6}$, car $30 = 8 \times 3 + 6$. Voici toute la table, chaque classe notée par son reste :

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Ces règles de calcul ont un nom, que tu verras au chapitre des structures.

Attention : Un produit nul modulo 8

Dans $\mathbb{Z}/8\mathbb{Z}$, $\overline{2} \times \overline{4} = \overline{0}$, alors que $\overline{2} \neq \overline{0}$ et $\overline{4} \neq \overline{0}$. Même $\overline{4} \times \overline{4} = \overline{0}$. La règle « un produit nul a un facteur nul » est fausse modulo un entier composé. N'en conclus rien sans un module premier.

Les classes inversibles

Relis la table : $\overline{1}$ apparaît dans les lignes de $\overline{1}, \overline{3}, \overline{5}$ et $\overline{7}$, jamais dans celles de $\overline{2}, \overline{4}, \overline{6}$. Par exemple, $\overline{3} \times \overline{3} = \overline{9} = \overline{1}$. Or $1, 3, 5$ et 7 sont exactement les restes premiers avec 8. **Pourquoi est-ce vrai ?** Trouver u tel que $au \equiv 1\ [n]$, c'est écrire $au + nv = 1$: on reconnaît Bézout.

Propriété : Classes inversibles de $\mathbb{Z}$/n$\mathbb{Z}$

Soient n un entier naturel, $n \geq 2$, et a un entier relatif. La classe $\overline{a}$ est **inversible** dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire qu'il existe une classe $\overline{b}$ telle que $\overline{a} \times \overline{b} = \overline{1}$, si et seulement si $a \wedge n = 1$.

Démonstration

Étape 1. Comme $\overline{a} \times \overline{b} = \overline{ab}$ (« Opérations dans $\mathbb{Z}$/n$\mathbb{Z}$ »), l'égalité $\overline{a} \times \overline{b} = \overline{1}$ équivaut à $ab \equiv 1\ [n]$ (« Description de $\mathbb{Z}$/n$\mathbb{Z}$ »), c'est-à-dire à l'existence d'un entier relatif k tel que $ab - 1 = nk$, soit $ab + n(-k) = 1$.

Étape 2. Donc $\overline{a}$ est inversible si et seulement s'il existe deux entiers relatifs u et v tels que $au + nv = 1$: si $\overline{a} \times \overline{b} = \overline{1}$, on prend $u = b$ et $v = -k$; si $au + nv = 1$, alors $au \equiv 1\ [n]$ et $\overline{a} \times \overline{u} = \overline{1}$.

Étape 3. Par le théorème de Bézout, cette dernière condition équivaut à $a \wedge n = 1$.

Méthode : inverser une classe

Montrer que $\overline{17}$ est inversible dans $\mathbb{Z}/40\mathbb{Z}$, puis trouver son inverse.

1. **Vérifier le PGCD.** $40 = 2 \times 17 + 6$, $17 = 2 \times 6 + 5$, $6 = 1 \times 5 + 1$. Le dernier reste non nul est 1, donc $17 \wedge 40 = 1$: $\overline{17}$ est inversible.
2. **Remonter les divisions.** $1 = 6 - 5 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17 = 3 \times 40 - 7 \times 17$.
3. **Conclure.** $17 \times (-7) \equiv 1\ [40]$, donc l'inverse de $\overline{17}$ est $\overline{-7} = \overline{33}$.
4. **Contrôler.** $17 \times 33 = 561 = 14 \times 40 + 1$.

Rédaction attendue. « $17 \wedge 40 = 1$, donc $\overline{17}$ est inversible (classes inversibles). Comme $17 \times (-7) + 40 \times 3 = 1$, l'inverse de $\overline{17}$ est $\overline{33}$. »

Vérifie : Une classe sans inverse

Laquelle de ces classes n'est **pas** inversible dans $\mathbb{Z}/15\mathbb{Z}$?

A. $\overline{2}$

Faux.
$2 \wedge 15 = 1$: elle est inversible, d'inverse $\overline{8}$, car $2 \times 8 = 16 \equiv 1\ [15]$.

B. $\overline{7}$

Faux.
$7 \wedge 15 = 1$: $7 \times 13 = 91 = 6 \times 15 + 1$, donc $\overline{13}$ est son inverse.

C. $\overline{14}$

Faux.
$14 \wedge 15 = 1$: $\overline{14} = \overline{-1}$ est son propre inverse, car $(-1) \times (-1) = 1$.

D. $\overline{9}$

Juste.
$9 \wedge 15 = 3 \neq 1$: d'après la caractérisation des classes inversibles, $\overline{9}$ n'a pas d'inverse.

Indice 1
Une classe $\overline{a}$ est inversible dans $\mathbb{Z}/15\mathbb{Z}$ si et seulement si $a \wedge 15 = 1$.

Indice 2
Cherche un diviseur commun à a et à 15, autre que 1.

Correction
$15 = 3 \times 5$. Parmi 2, 7, 14 et 9, seul 9 est divisible par 3 ou par 5 : $9 \wedge 15 = 3$. Donc $\overline{9}$ n'est pas inversible (classes inversibles de $\mathbb{Z}/n\mathbb{Z}$). D'ailleurs $\overline{9} \times \overline{5} = \overline{45} = \overline{0}$, avec $\overline{5} \neq \overline{0}$.

Un module premier

Propriété : Le cas de $\mathbb{Z}$/p$\mathbb{Z}$, p premier

Soit p un nombre premier.

1. Toute classe non nulle de $\mathbb{Z}/p\mathbb{Z}$ est inversible.
2. Pour toutes classes $\overline{a}$ et $\overline{b}$ de $\mathbb{Z}/p\mathbb{Z}$: si $\overline{a} \times \overline{b} = \overline{0}$, alors $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Démonstration

Étape 1 (point 1). Si $\overline{a} \neq \overline{0}$, alors $a \not\equiv 0\ [p]$ (« Description de $\mathbb{Z}$/n$\mathbb{Z}$ »), c'est-à-dire $p \nmid a$. D'après « Conséquences du théorème de Gauss » (point 1), $a \wedge p = 1$, donc $\overline{a}$ est inversible (« Classes inversibles de $\mathbb{Z}$/n$\mathbb{Z}$ »).

Étape 2 (point 2). Si $\overline{a} \times \overline{b} = \overline{0}$, alors $\overline{ab} = \overline{0}$ (« Opérations dans $\mathbb{Z}$/n$\mathbb{Z}$ »), donc $ab \equiv 0\ [p]$ (« Description de $\mathbb{Z}$/n$\mathbb{Z}$ »), c'est-à-dire $p \mid ab$. D'après « Conséquences du théorème de Gauss » (point 2), $p \mid a$ ou $p \mid b$, soit $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Exemple : La table de multiplication de $\mathbb{Z}/5\mathbb{Z}$

Modulo 5, nombre premier, chaque ligne non nulle contient $\overline{1}$, et aucun produit de deux classes non nulles n'est nul :

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On y lit les inverses : $\overline{1}$ et $\overline{4}$ sont leurs propres inverses ; $\overline{2}$ et $\overline{3}$ sont inverses l'un de l'autre.

Petit théorème de Fermat

Observer des restes

Calculer le reste de 5^{2026} dans la division par 11, sans calculatrice ni patience infinie : voilà ce que permet le petit théorème de Fermat. Il sert dans 11 des 13 exercices d'arithmétique consultés. Tout part d'une observation sur des restes.

Devine : Les multiples de 3 modulo 11

On écrit les dix entiers $3, 6, 9, \ldots, 30$, puis leurs restes dans la division par 11. Combien de restes **différents** obtient-on ?

A. 10

Juste.
Les restes sont $3, 6, 9, 1, 4, 7, 10, 2, 5, 8$: chaque entier de 1 à 10 apparaît une fois.

B. 11

Faux.
Il n'y a que dix entiers, donc au plus dix restes. Et le reste 0 n'apparaît pas : aucun de ces entiers n'est multiple de 11.

C. 9

Faux.
Tu as supposé que deux restes se répètent, ou que le reste 0 apparaît. Calcule-les : aucun n'est nul, et ils sont tous distincts.

Indice 1
Calcule $3k$ pour $k = 1, \ldots, 10$, puis retire 11 autant de fois que possible.
Indice 2
Par exemple, $12 = 11 + 1$ donne le reste 1.

Correction

k	1	2	3	4	5	6	7	8	9	10
$3k$	3	6	9	12	15	18	21	24	27	30
reste	3	6	9	1	4	7	10	2	5	8

Les dix restes sont $1, 2, \ldots, 10$, chacun une fois, dans le désordre.

Ce que tu viens d'observer pour 3 et 11 vaut-il pour tout premier p et tout entier a que p ne divise pas ? L'énoncé suivant l'affirme. **Pourquoi est-ce vrai** ? La preuve, sous l'énoncé, répond à deux questions. Un multiple ka peut-il être divisible par p ? Deux multiples distincts peuvent-ils avoir le même reste ?

Le lemme des multiples

Propriété : Multiples d'un entier modulo p

Soient p un nombre premier et a un entier relatif tel que $p \nmid a$. Les restes, dans la division euclidienne par p, des $p-1$ entiers

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

sont les entiers $1, 2, \ldots, p-1$, chacun exactement une fois.

Démonstration

Étape 1 (aucun reste nul). Soit k un entier tel que $1 \leq k \leq p-1$. Alors $p \nmid k$ (« Propriétés de la divisibilité », point 3) et $p \nmid a$, donc $p \nmid ka$ (« Conséquences du théorème de Gauss », point 2) : le reste de ka n'est pas nul (« Congruence et reste »).

Étape 2 (restes distincts). Supposons que ka et la aient le même reste, avec $1 \leq l < k \leq p-1$. Alors $ka \equiv la\ [p]$ (« Congruence et reste »), donc $p \mid (k-l)a$. Comme $a \wedge p = 1$ (« Conséquences du théorème de Gauss », point 1), le théorème de Gauss donne $p \mid k-l$. Or $0 < k-l < p$: c'est impossible (« Propriétés de la divisibilité », point 3).

Étape 3. Les $p-1$ restes sont deux à deux distincts et appartiennent à $\{1, 2, \ldots, p-1\}$, qui a $p-1$ éléments. Ils sont donc exactement $1, 2, \ldots, p-1$.

À retenir : Ce qu'il faut retenir de la preuve

Pour montrer que $p-1$ restes sont exactement $1, 2, \ldots, p-1$, on ne les calcule pas. On montre qu'ils sont **non nuls** et **deux à deux distincts**, puis on compte : $p-1$ valeurs distinctes dans un ensemble à $p-1$ éléments les prennent toutes.

Vérifie : L'argument de l'étape 2

Dans la preuve, on arrive à $p \mid (k-l)a$. Quel argument permet d'en déduire $p \mid k-l$?

A. Le petit théorème de Fermat.

Faux.
Fermat se démontre **à partir** de ce lemme : l'utiliser ici serait un raisonnement circulaire.

B. Le théorème de Gauss, car $a \wedge p = 1$.

Juste.

p divise le produit $(k-l)a$ et p est premier avec a (conséquences du théorème de Gauss, point 1, car $p \nmid a$) : Gauss donne $p \mid k-l$.

C. L'encadrement $0 < k-l < p$.

Faux.

Cet encadrement sert juste après, pour obtenir une contradiction. Il ne transforme pas $p \mid (k-l)a$ en $p \mid k-l$.

Indice 1

On cherche à « enlever » le facteur a d'une divisibilité.

Indice 2

Quel théorème fait passer de $p \mid bc$ à $p \mid c$, et sous quelle hypothèse ?

Correction

On a $p \mid (k-l)a$. Comme p est premier et $p \nmid a$, on a $a \wedge p = 1$ (conséquences du théorème de Gauss, point 1). Le théorème de Gauss donne alors $p \mid k-l$. L'encadrement $0 < k-l < p$ rend cette divisibilité impossible : deux restes ne sont jamais égaux.

Exemple : Contre-exemple : un facteur commun

Prends le module 9 et $a = 6$, qui ont le facteur 3 en commun. Les restes de $6, 12, 18, \ldots, 48$ modulo 9 sont :

$$6,\ 3,\ 0,\ 6,\ 3,\ 0,\ 6,\ 3.$$

Le reste 0 apparaît, et les restes se répètent. Avec un premier p tel que $p \nmid a$, on a $a \wedge p = 1$: c'est exactement ce qui manque ici.

Le petit théorème de Fermat

Reprends $a = 3$ et $p = 11$. Le produit des dix entiers $3, 6, \ldots, 30$ vaut $3^{10} \times 10!$, où $10! = 1 \times 2 \times \cdots \times 10$.

Ce produit est congru modulo 11 au produit des restes, qui sont $1, 2, \ldots, 10$ dans le désordre. Donc

$$3^{10} \times 10! \equiv 10! \ [11].$$

Si l'on peut « simplifier » par $10!$, on obtient $3^{10} \equiv 1 \ [11]$. Vérifie : $3^5 = 243 = 22 \times 11 + 1$, donc $3^{10} \equiv 1 \ [11]$.

Pourquoi est-ce vrai pour tout premier ? C'est le théorème suivant.

Théorème : Petit théorème de Fermat

Soit p un nombre premier.

1. Pour tout entier relatif a tel que $p \nmid a$: $a^{p-1} \equiv 1 \ [p]$.
2. Pour tout entier relatif a : $a^p \equiv a \ [p]$.

Démonstration

Étape 1. Soit a tel que $p \nmid a$. On note $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$. Chaque ka, pour $1 \leq k \leq p-1$, est congru à son reste (« Congruence et reste ») ; d'après « Multiples d'un entier modulo p », ces restes sont $1, 2, \ldots, p-1$ dans un autre ordre. En multipliant ces $p-1$ congruences une à une (« Opérations sur les congruences », point 2, de proche en proche) :

$$a \times 2a \times \cdots \times (p-1)a \equiv (p-1)! \ [p], \quad \text{soit} \quad a^{p-1}\,(p-1)! \equiv (p-1)! \ [p].$$

Étape 2. Donc $p \mid (p-1)!\,(a^{p-1}-1)$. Aucun des facteurs $1, \ldots, p-1$ n'est divisible par p (« Propriétés de la divisibilité », point 3), donc $p \nmid (p-1)!$ (« Conséquences du théorème de Gauss », point 4), puis $(p-1)! \wedge p = 1$ (« Conséquences du théorème de Gauss », point 1). Le théorème de Gauss donne $p \mid a^{p-1}-1$: c'est le point 1.

Étape 3 (point 2). Si $p \nmid a$, on multiplie le point 1 par a (« Opérations sur les congruences »). Si $p \mid a$, alors $a \equiv 0 \ [p]$, donc $a^p \equiv 0 \equiv a \ [p]$.

À retenir : Ce qu'il faut retenir de la preuve

On multiplie les $p-1$ congruences du lemme : $a^{p-1} \times (p-1)! \equiv (p-1)! \ [p]$. Puis on « simplifie » par $(p-1)!$: toute la question est de savoir pourquoi on en a le droit. Le point 2 s'en déduit en séparant les cas $p \nmid a$ et $p \mid a$.

Vérifie : La simplification de l'étape 2

Dans la preuve, on obtient $p \mid (p-1)!\,(a^{p-1}-1)$. Pourquoi a-t-on le droit d'en déduire $p \mid a^{p-1}-1$?

A. Parce que $(p-1)! \neq 0$.

Faux.
Un facteur non nul ne suffit pas : $6 \mid 2 \times 3$, et pourtant $6 \nmid 3$. Il faut un facteur premier avec le diviseur.

B. Parce que $(p-1)! \equiv 1 \ [p]$.

Faux.
C'est faux en général : pour $p = 5$, $4! = 24 \equiv 4 \ [5]$.

C. Parce que $(p-1)! \wedge p = 1$, puis par le théorème de Gauss.

Juste.
Aucun des facteurs $1, \ldots, p-1$ n'est divisible par p, donc $p \nmid (p-1)!$, puis $(p-1)! \wedge p = 1$: Gauss s'applique.

D. Par le petit théorème de Fermat.

Faux.
C'est ce qu'on est en train de démontrer : le raisonnement serait circulaire.

Indice 1
Simplifier une divisibilité par un facteur, c'est appliquer Gauss.
Indice 2
Gauss exige que ce facteur soit premier avec p.

Correction
p ne divise aucun des entiers $1, 2, \dots, p-1$. Comme p est premier, il ne divise pas leur produit (conséquences du théorème de Gauss, point 4). Donc $(p-1)! \wedge p = 1$ (même énoncé, point 1). Le théorème de Gauss donne $p \mid a^{p-1} - 1$.

Exemple : Contre-exemple : un module composé

Le théorème exige un module **premier**. Avec 15, composé, et $a = 2$, premier avec 15 :
$2^4 = 16 \equiv 1\ [15]$, donc

$$2^{14} = (2^4)^3 \times 2^2 \equiv 4\ [15].$$

On n'a donc pas $2^{15-1} \equiv 1\ [15]$: sans module premier, la conclusion peut être fausse.

Réduire l'exposant

Méthode : Fermat et réduction de l'exposant

Montrer que le reste de 5^{2026} dans la division par 11 est 5.

1. **Hypothèses.** 11 est premier et $11 \nmid 5$. D'après le petit théorème de Fermat, $5^{10} \equiv 1\ [11]$.
2. **Diviser l'exposant par $p-1 = 10$.** $2026 = 10 \times 202 + 6$, avec $0 \leq 6 < 10$.
3. **Réduire.** $5^{2026} = (5^{10})^{202} \times 5^6 \equiv 1^{202} \times 5^6\ [11]$.
4. **Finir le calcul.** $5^2 = 25 \equiv 3\ [11]$, donc $5^6 \equiv 3^3 = 27 \equiv 5\ [11]$.
5. **Conclure.** $5^{2026} \equiv 5\ [11]$ et $0 \leq 5 < 11$: le reste est 5.

Rédaction attendue. « 11 est premier et $11 \nmid 5$: d'après le petit théorème de Fermat, $5^{10} \equiv 1\ [11]$. » Le module s'écrit à chaque ligne.

À toi : un reste par Fermat

Détermine le reste de 2^{100} dans la division par 13. Rédige en citant les hypothèses du petit théorème de Fermat.

Indice 1
Écris les hypothèses : 13 est premier, et 13 ne divise pas 2.
Indice 2
Fermat donne $2^{12} \equiv 1\ [13]$: divise 100 par 12.

Indice 3
Il reste à calculer 2^4 modulo 13.

Réponse
Hypothèses. 13 est premier et $13 \nmid 2$. D'après le petit théorème de Fermat, $2^{12} \equiv 1\ [13]$.

Réduire l'exposant. Or $100 = 12 \times 8 + 4$, avec $0 \leq 4 < 12$. Donc

$$\begin{aligned} 2^{100} &= (2^{12})^8 \times 2^4 \\ &\equiv 1^8 \times 16\ [13]. \end{aligned}$$

Conclusion. Comme $16 = 13 \times 1 + 3$, on a $2^{100} \equiv 3\ [13]$, avec $0 \leq 3 < 13$: le reste de 2^{100} dans la division par 13 est 3.

Attention : Fermat sans l'hypothèse p ∤ a

Avec $p = 5$ et $a = 35$: $35 \equiv 0\ [5]$, donc $35^4 \equiv 0\ [5]$, et non 1. Avant d'écrire $a^{p-1} \equiv 1\ [p]$, écris toujours « p est premier et $p \nmid a$ ». La forme $a^p \equiv a\ [p]$, elle, vaut pour tout entier a.

À toi : Coin examen

Montrer que 30 divise $a^5 - a$ pour tout entier a. *(2 points, barème indicatif BURHAN.)*

Indice 1
$30 = 2 \times 3 \times 5$: montre que 2, 3 et 5 divisent $a^5 - a$.
Indice 2
Pour chaque premier p, utilise la forme $a^p \equiv a\ [p]$ du petit théorème de Fermat : elle vaut pour tout entier a.
Indice 3
Pour assembler, nomme la primalité relative : conséquences du théorème de Gauss, point 3.

Réponse
Rédaction attendue.

- 5 est premier : d'après le petit théorème de Fermat (point 2), $a^5 \equiv a\ [5]$. **0,5 pt**
- 3 est premier : $a^3 \equiv a\ [3]$, donc $a^5 = a^3 \times a^2 \equiv a \times a^2 = a^3 \equiv a\ [3]$. **0,5 pt**
- 2 est premier : $a^2 \equiv a\ [2]$, donc $a^5 = (a^2)^2 \times a \equiv a^2 \times a \equiv a \times a \equiv a\ [2]$. **0,25 pt**
- 2 et 3 divisent $a^5 - a$ et $2 \wedge 3 = 1$, donc $6 \mid a^5 - a$ (conséquences du théorème de Gauss, point 3). De même, $6 \wedge 5 = 1$ donne $30 \mid a^5 - a$. **0,75 pt**

Équation ax + by = c

Existe-t-il des solutions

Devine : Un total impossible ?

On cherche des entiers relatifs x et y tels que $6x + 15y = 50$. Quel raisonnement est juste ?

A. Aucune solution, car $6x + 15y$ est toujours un multiple de 3, et 50 ne l'est pas.

Juste.

3 divise 6 et 15, donc 3 divise $6x + 15y$ (propriétés de la divisibilité, point 2). Or $3 \nmid 50$.

B. Il y a des solutions, car $6 \wedge 15 \neq 0$.

Faux.

Le PGCD n'est jamais nul ici. Ce qui compte, c'est de savoir s'il divise 50.

C. Aucune solution, car 50 n'est multiple ni de 6 ni de 15.

Faux.

Ce raisonnement ne vaut rien : 21 n'est multiple ni de 6 ni de 15, et pourtant $6 \times 1 + 15 \times 1 = 21$.

Indice 1

Cherche un entier qui divise à coup sûr $6x + 15y$, quels que soient x et y.

Indice 2

Calcule $6 \wedge 15$.

Correction

$6 \wedge 15 = 3$. Pour tous entiers x et y, 3 divise $6x + 15y$. Comme $50 = 3 \times 16 + 2$, $3 \nmid 50$: l'équation n'a aucune solution. L'énoncé suivant dit que ce test du PGCD suffit toujours.

Théorème : Existence de solutions de ax + by = c

Soient a et b deux entiers relatifs non nuls, c un entier relatif et $d = a \wedge b$. L'équation $ax + by = c$, d'inconnue $(x, y) \in \mathbb{Z}^2$, admet au moins une solution si et seulement si $d \mid c$.

Démonstration

Sens direct. Si (x, y) est une solution, alors $d \mid a$ et $d \mid b$, donc $d \mid ax + by = c$ (« Propriétés de la divisibilité », point 2).

Réciproque. Si $d \mid c$, on écrit $c = dk$ avec $k \in \mathbb{Z}$. L'identité de Bézout donne u et v tels que $au + bv = d$. En multipliant par k : $a(uk) + b(vk) = c$. Le couple (uk, vk) est une solution.

Exemple : Deux équations voisines

On a $15 \wedge 21 = 3$.

- $15x + 21y = 9$: $3 \mid 9$, donc il y a des solutions, d'après l'existence de solutions de $ax + by = c$. Par exemple, $15 \times 2 + 21 \times (-1) = 9$.
- $15x + 21y = 10$: $3 \nmid 10$, donc il n'y en a aucune.

Les coefficients sont les mêmes : seul le second membre décide.

Attention : Bézout ne fabrique pas n'importe quel second membre

Pour $10x + 15y = 8$, on lit parfois : « par Bézout, il existe u et v, donc il y a une solution ». C'est faux. Bézout donne $10u + 15v = 5$, le PGCD, et non 8. Ici $5 \nmid 8$: aucune solution. Calcule toujours $d = a \wedge b$ et teste $d \mid c$ **avant** de chercher une solution.

Toutes les solutions

Pour $5x + 8y = 3$, le couple $(-1, 1)$ convient : $-5 + 8 = 3$. Ajoute 8 à x et retire 5 à y : $(7, -4)$ convient aussi, car $35 - 32 = 3$. On peut recommencer sans fin. **Pourquoi est-ce vrai**, et pourquoi n'y a-t-il pas d'autres solutions ? Le théorème suivant répond, grâce à Gauss.

Théorème : Solutions de ax + by = c

Soient a et b deux entiers relatifs non nuls et premiers entre eux, c un entier relatif, et (x_0, y_0) une solution de l'équation $ax + by = c$ dans $\mathbb{Z}^2$. Les solutions de cette équation dans $\mathbb{Z}^2$ sont exactement les couples

$$(x_0 + bk,\ y_0 - ak), \quad k \in \mathbb{Z}.$$

Démonstration

Étape 1 (ces couples sont des solutions). Pour tout $k \in \mathbb{Z}$: $a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 = c$.

Étape 2 (il n'y en a pas d'autres). Soit (x, y) une solution. Par différence avec $ax_0 + by_0 = c$: $a(x - x_0) = b(y_0 - y)$. Donc $b \mid a(x - x_0)$. Comme $b \wedge a = 1$, le théorème de Gauss donne $b \mid x - x_0$: il existe $k \in \mathbb{Z}$ tel que $x = x_0 + bk$.

Étape 3. En reportant : $abk = b(y_0 - y)$. Comme $b \neq 0$, on simplifie par b : $y_0 - y = ak$, soit $y = y_0 - ak$.

À retenir : Ce qu'il faut retenir de la preuve

Deux solutions d'une même équation se soustraient : $a(x - x_0) = b(y_0 - y)$. Le théorème de Gauss donne alors $b \mid x - x_0$. Retiens ce réflexe : **soustraire, puis Gauss**.

Vérifie : L'hypothèse qui fait tout

À l'étape 2 de la preuve, quelle hypothèse permet d'appliquer le théorème de Gauss à $b \mid a(x - x_0)$?

A. $b \neq 0$

Faux.

Elle sert à l'étape 3, pour simplifier $abk = b(y_0 - y)$ par b.

B. $a \wedge b = 1$

Juste.

Gauss demande que b soit premier avec le facteur a : c'est exactement l'hypothèse $a \wedge b = 1$.

C. $c \neq 0$

Faux.

L'énoncé ne suppose rien sur c : la preuve marche aussi pour $c = 0$.

Indice 1

Rappelle-toi Gauss : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Indice 2

Ici, le diviseur est b et le facteur à « enlever » est a.

Correction

On a $b \mid a(x - x_0)$. Le théorème de Gauss en déduit $b \mid x - x_0$ à condition que $b \wedge a = 1$: c'est l'hypothèse « a et b premiers entre eux » du théorème. L'hypothèse $b \neq 0$ sert ensuite, à l'étape 3.

Exemple : Contre-exemple : sans diviser par d

Pour $18x + 30y = 24$, on a $18 \wedge 30 = 6 \neq 1$. Le couple $(3, -1)$ est solution : $54 - 30 = 24$.

Appliquer tel quel le théorème des solutions donnerait les couples $(3 + 30k,\ -1 - 18k)$. On oublierait $(-2, 2)$, qui est solution : $-36 + 60 = 24$.

Il faut d'abord diviser par 6 : $3x + 5y = 4$. Ses solutions sont les couples $(3 + 5k,\ -1 - 3k)$, $k \in \mathbb{Z}$.

La méthode complète

Méthode : résoudre ax + by = c

Résoudre dans $\mathbb{Z}^2$ l'équation $33x + 24y = 15$.

1. **PGCD.** $33 = 1 \times 24 + 9$, $24 = 2 \times 9 + 6$, $9 = 1 \times 6 + 3$, $6 = 2 \times 3$. Donc $33 \wedge 24 = 3$, et $3 \mid 15$: il y a des solutions.
2. **Simplifier.** On divise par 3 : $11x + 8y = 5$, avec $11 \wedge 8 = 1$.
3. **Solution particulière.** La remontée d'Euclide donne un couple de Bézout : $11 \times 3 + 8 \times (-4) = 1$. En multipliant par 5 : $11 \times 15 + 8 \times (-20) = 5$. Ici, une solution plus simple se voit : $11 \times (-1) + 8 \times 2 = 5$. On prend $(x_0, y_0) = (-1, 2)$.
4. **Conclure** avec $a = 11$ et $b = 8$: les solutions sont les couples $(-1 + 8k,\ 2 - 11k)$, $k \in \mathbb{Z}$.

Rédaction attendue. « $11 \wedge 8 = 1$ et $(-1, 2)$ est solution. D'après le théorème des solutions de $ax + by = c$, les solutions sont les couples $(-1 + 8k,\ 2 - 11k)$, avec $k \in \mathbb{Z}$. »

À toi : À toi de résoudre

Résous dans $\mathbb{Z}^2$ l'équation $9x + 4y = 2$.

Indice 1
Calcule $9 \wedge 4$: faut-il simplifier ?
Indice 2
Pars d'un couple de Bézout : $9 \times 1 + 4 \times (-2) = 1$, puis multiplie par 2.
Indice 3
Applique le théorème des solutions avec $a = 9$ et $b = 4$: attention à l'ordre des coefficients.

Réponse
Existence. $9 \wedge 4 = 1$ et $1 \mid 2$: il y a des solutions, sans simplification.

Solution particulière. On a $9 \times 1 + 4 \times (-2) = 1$. En multipliant par 2, $9 \times 2 + 4 \times (-4) = 2$, donc $(x_0, y_0) = (2, -4)$.

Conclusion. D'après le théorème des solutions de $ax + by = c$, les solutions de $9x + 4y = 2$ dans $\mathbb{Z}^2$ sont les couples $(2 + 4k,\ -4 - 9k)$, $k \in \mathbb{Z}$.

Contrôle avec $k = 1$: $9 \times 6 + 4 \times (-13) = 54 - 52 = 2$.

Exemple **: Coin examen**

La partie « il n'y a pas d'autres solutions » se rédige ainsi, pour $11x + 8y = 5$. Points indicatifs, barème BURHAN.

- Soit (x, y) une solution. Par différence avec $11 \times (-1) + 8 \times 2 = 5$: $11(x + 1) = 8(2 - y)$. **0,25 pt**
- Donc $8 \mid 11(x + 1)$. Or $8 \wedge 11 = 1$: d'après le théorème de Gauss, $8 \mid x + 1$. **0,5 pt**
- On écrit $x = -1 + 8k$, $k \in \mathbb{Z}$. Alors $88k = 8(2 - y)$, d'où $y = 2 - 11k$. **0,5 pt**
- Réciproquement, ces couples conviennent : $11(-1 + 8k) + 8(2 - 11k) = 5$. **0,25 pt**

Numération en base b

Écrire un entier en base b

Devine : Un nombre en base deux

En base deux, on n'utilise que les chiffres 0 et 1. Quel entier l'écriture $\overline{1011}^{(2)}$ représente-t-elle ?

A. 1011

Faux.

C'est la lecture en base dix. Ici, chaque position vaut une puissance de 2, pas de 10.

B. 13

Faux.

Tu as lu les chiffres de droite à gauche : $\overline{1101}^{(2)} = 13$. Le chiffre de droite est celui des unités.

C. 3

Faux.

Tu as compté les chiffres 1. Chaque 1 vaut une puissance de 2, qui dépend de sa place.

D. 11

Juste.

$1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1 = 8 + 2 + 1 = 11$.

Indice 1

En base dix, $1011 = 1 \times 10^3 + 0 \times 10^2 + 1 \times 10 + 1$.

Indice 2

Remplace 10 par 2.

Correction

$\overline{1011}^{(2)} = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1 = 8 + 0 + 2 + 1 = 11$.

En base dix, $2075 = 2 \times 10^3 + 0 \times 10^2 + 7 \times 10 + 5$: chaque chiffre multiplie une puissance de 10. En **base** b, on fait de même avec les puissances de b, et les **chiffres** vont de 0 à $b - 1$. Pour ne pas confondre avec une classe de $\mathbb{Z}/n\mathbb{Z}$, on écrit toujours l'exposant (b). Sous l'énoncé, tu trouveras une idée de la preuve, sans tous les détails.

Théorème : Écriture en base b

Soit b un entier naturel, $b \geq 2$. Tout entier naturel non nul n s'écrit de manière unique sous la forme

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

où k est un entier naturel et où les **chiffres** $a_0, a_1, \ldots, a_k$ sont des entiers tels que $0 \leq a_i \leq b - 1$ et $a_k \neq 0$. On note $n = \overline{a_k a_{k-1} \ldots a_1 a_0}^{(b)}$.

Démonstration

Idée de la preuve.

Existence. On divise n par b : $n = bq_0 + a_0$ avec $0 \leq a_0 \leq b - 1$ (« Division euclidienne dans $\mathbb{Z}$ »). On divise ensuite q_0 par b, et ainsi de suite. Les quotients successifs forment une suite strictement décroissante d'entiers naturels tant qu'ils sont non nuls : l'un d'eux s'annule. Les restes successifs $a_0, a_1, \ldots, a_k$ sont les chiffres ; le dernier, a_k, est le dernier quotient non nul, donc $a_k \neq 0$.

Unicité. Dans une écriture $n = (a_k b^{k-1} + \cdots + a_1)b + a_0$ avec $0 \leq a_0 \leq b-1$, le chiffre a_0 est le reste de la division de n par b (unicité dans « Division euclidienne dans $\mathbb{Z}$ »). On recommence avec le quotient ; l'unicité des restes successifs donne aussi celle de k.

Étape omise : la récurrence qui formalise « et ainsi de suite ».

Exemple : De la base huit vers la base dix

$\overline{257}^{(8)} = 2 \times 8^2 + 5 \times 8 + 7 = 128 + 40 + 7 = 175$. On développe selon les puissances de la base, du chiffre de gauche jusqu'au chiffre des unités.

Changer de base

Méthode : de la base dix vers la base b

Écrire 2026 en base 5. On divise par 5 jusqu'à obtenir un quotient nul, chaque reste vérifiant $0 \leq r < 5$:

$$\begin{aligned} 2026 &= 5 \times 405 + 1 \\ 405 &= 5 \times 81 + 0 \\ 81 &= 5 \times 16 + 1 \\ 16 &= 5 \times 3 + 1 \\ 3 &= 5 \times 0 + 3 \end{aligned}$$

On lit les restes **du dernier au premier** : $2026 = \overline{31101}^{(5)}$. **Contrôle** : $3 \times 625 + 1 \times 125 + 1 \times 25 + 0 \times 5 + 1 = 2026$.

Attention : Un chiffre trop grand

En base 5, les seuls chiffres sont $0, 1, 2, 3$ et 4. L'écriture $\overline{1352}^{(5)}$ n'a donc aucun sens : 5 n'est pas un chiffre en base 5. Si une division te donne un « reste » égal ou supérieur à b, elle est fausse : recommence-la.

À toi : Vers la base quatre

Quelle est l'écriture de 95 en base 4 ?

A. $\overline{3311}^{(4)}$

Faux.
Tu as écrit les restes dans l'ordre où ils sont apparus. Le premier reste obtenu est le chiffre des unités : il s'écrit à droite.

B. $\overline{533}^{(4)}$

Faux.

Tu t'es arrêté trop tôt : 5 n'est pas un chiffre en base 4. Il faut encore diviser 5 par 4.

C. $\overline{1133}^{(4)}$

Juste.

$1 \times 64 + 1 \times 16 + 3 \times 4 + 3 = 95$.

Indice 1

Divise 95 par 4, puis le quotient par 4, et ainsi de suite.

Indice 2

Le premier reste obtenu est le chiffre des unités.

Correction

$95 = 4 \times 23 + 3$, $23 = 4 \times 5 + 3$, $5 = 4 \times 1 + 1$, $1 = 4 \times 0 + 1$. Les restes, lus du dernier au premier, donnent $95 = \overline{1133}^{(4)}$. Contrôle : $64 + 16 + 12 + 3 = 95$.

Calculer en base b

Exemple : Une addition en base cinq

On pose $\overline{243}^{(5)} + \overline{132}^{(5)}$ comme en base dix, mais la retenue part dès qu'on atteint 5 :

- unités : $3 + 2 = 5 = \overline{10}^{(5)}$; on écrit 0 et on retient 1 ;
- rang suivant : $4 + 3 + 1 = 8 = \overline{13}^{(5)}$; on écrit 3 et on retient 1 ;
- dernier rang : $2 + 1 + 1 = 4$.

Résultat : $\overline{430}^{(5)}$. Contrôle en base dix : $73 + 42 = 115 = 4 \times 25 + 3 \times 5$.

À toi : Divisible sans convertir

Sans convertir en base dix, montre que $\overline{4321}^{(6)}$ est divisible par 5.

Indice 1

Quel est le reste de 6 dans la division par 5 ?

Indice 2

Puisque $6 \equiv 1\ [5]$, chaque puissance 6^k est congrue à 1 modulo 5 (opérations sur les congruences).

Réponse

On a $6 \equiv 1\ [5]$, donc $6^k \equiv 1\ [5]$ pour tout entier naturel k (opérations sur les congruences, point 3).

Ainsi

$$\begin{aligned}\overline{4321}^{(6)} &= 4 \times 6^3 + 3 \times 6^2 \\ &\quad + 2 \times 6 + 1 \\ &\equiv 4 + 3 + 2 + 1 \\ &= 10 \equiv 0\ [5].\end{aligned}$$

Conclusion. 5 divise $\overline{4321}^{(6)}$. Contrôle : $\overline{4321}^{(6)} = 985 = 5 \times 197$.

C'est l'argument du critère de divisibilité par 9 en base dix, où $10 \equiv 1\ [9]$.

La chaîne d'examen : un premier p générique

Te voilà au bout du chapitre. Un exercice d'arithmétique figure dans 13 des 16 sujets consultés (2017-2022 et 2024-2025). **À maîtriser** : une chaîne de raisonnement sur un premier p quelconque. Primalité relative, Fermat, congruence, conclusion. On l'entraîne ici sur un objet neuf, après un dernier outil : le plus petit diviseur premier.

Méthode : raisonner avec le plus petit diviseur premier

Montrer que, si p est le plus petit diviseur premier d'un entier $n \geq 2$, tout entier k tel que $2 \leq k \leq p-1$ vérifie $k \wedge n = 1$.

1. **Supposer le contraire.** Soit $d = k \wedge n$. Supposons par l'absurde que $d \geq 2$.
2. **Introduire un premier.** d admet un diviseur premier p' (propriété du plus petit diviseur premier). Alors $p' \mid d$ et $d \mid n$, donc $p' \mid n$.
3. **Utiliser la minimalité.** $p' \leq d \leq k \leq p-1$: p' serait un diviseur premier de n plus petit que p. C'est absurde, donc $d = 1$.

Exemple : $899 = 29 \times 31$ a pour plus petit diviseur premier 29. Chacun des entiers $2, 3, \ldots, 28$ est donc premier avec 899.

Vérifie : Premier avec 391 ?

Le plus petit diviseur premier de 391 est 17. Lequel de ces entiers est **à coup sûr** premier avec 391, d'après la méthode ?

A. 16

Juste.
$2 \leq 16 \leq 17 - 1$: la méthode s'applique, donc $16 \wedge 391 = 1$.

B. 23

Faux.
$391 = 17 \times 23$: 23 divise 391, donc $23 \wedge 391 = 23$.

C. 34

Faux.
$34 = 2 \times 17$ partage le facteur 17 avec 391 : $34 \wedge 391 = 17$.

Indice 1
La méthode ne concerne que les entiers compris entre 2 et $p-1$.
Indice 2

Ici, $p = 17$.

Correction
La méthode donne : tout entier k tel que $2 \leq k \leq 16$ est premier avec 391. C'est le cas de 16. En revanche, $391 = 17 \times 23$: 23 et $34 = 2 \times 17$ ont un facteur commun avec 391.

Exemple : Coin examen : la chaîne

Soient p un nombre premier différent de 2, 3 et 5, et R l'entier qui s'écrit avec $p-1$ chiffres 1 en base dix. Points indicatifs, barème BURHAN.

- **Q1. Montrer que $p \wedge 10 = 1$.** Les seuls diviseurs premiers de 10 sont 2 et 5, et p n'est ni l'un ni l'autre : $p \nmid 10$. Comme p est premier, $p \wedge 10 = 1$ (conséquences du théorème de Gauss, point 1). **0,5 pt**
- **Q2. Montrer que $10^{p-1} \equiv 1\ [p]$.** p est premier et $p \nmid 10$: d'après le petit théorème de Fermat, $10^{p-1} \equiv 1\ [p]$. **0,5 pt**

Exemple : Coin examen : la conclusion

Q3. Montrer que $p \mid R$. On a

$$\begin{aligned} 9R &= 99\ldots9 \\ &= 10^{p-1} - 1, \end{aligned}$$

donc $p \mid 9R$ d'après Q2. Comme $p \neq 3$, $p \nmid 9$ et $p \wedge 9 = 1$. D'après le théorème de Gauss, $p \mid R$. **0,75 pt**

Q4. En déduire un couple de Bézout de 10 et p. D'après Q2, il existe un entier k tel que $10^{p-1} - 1 = kp$. Donc

$$\begin{aligned} &10 \times 10^{p-2} \\ &\quad + p \times (-k) = 1, \end{aligned}$$

et le couple $(10^{p-2}, -k)$ convient. **0,5 pt**

Application : pour $p = 11$,

$$\begin{aligned} R &= 1\,111\,111\,111 \\ &= 11 \times 101\,010\,101. \end{aligned}$$

À toi : Une application numérique

Quel est le reste de 10^{50} dans la division par 17 ?

A. 15
Juste.

$10^{50} \equiv 10^2\ [17]$, et $100 = 5 \times 17 + 15$.

B. 1

Faux.

Tu as réduit l'exposant modulo 17 : $50 = 2 \times 17 + 16$, puis $10^{16} \equiv 1\ [17]$. Mais Fermat réduit l'exposant modulo $p - 1 = 16$.

C. 2

Faux.

2 est le reste de l'exposant : $50 = 16 \times 3 + 2$. Il reste à calculer 10^2 modulo 17.

Indice 1

17 est premier et $17 \nmid 10$: écris la conclusion de Fermat.

Indice 2

Divise 50 par 16.

Correction

Hypothèses. 17 est premier et $17 \nmid 10$. D'après le petit théorème de Fermat, $10^{16} \equiv 1\ [17]$.

Réduire l'exposant. Or $50 = 16 \times 3 + 2$, avec $0 \leq 2 < 16$. Donc

$$\begin{aligned} 10^{50} &= (10^{16})^3 \times 10^2 \\ &\equiv 100\ [17]. \end{aligned}$$

Conclusion. Comme $100 = 5 \times 17 + 15$, avec $0 \leq 15 < 17$, le reste de 10^{50} dans la division par 17 est 15.

Le mot du prof. Tu sais maintenant enchaîner un premier quelconque, une primalité relative, Fermat et Gauss jusqu'à une conclusion propre. Garde des rédactions courtes, et nomme chaque hypothèse : c'est elle qui rapporte les points.

SOURCES

Référentiel BURHAN du chapitre « Arithmétique dans $\mathbb{Z}$ » (2bac · sciences-mathematiques · mathematiques)