BURHAN

Arithmétique dans $\mathbb{Z}$: Résumé

2ème Année Baccalauréat · Sciences Mathématiques · Mathématiques

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

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

L'essentiel en une page

Ce chapitre repose sur peu d'outils, mais chacun a ses conditions. Ce sont elles que le correcteur vérifie. On note $a \wedge b$ le PGCD de a et b, et $a \vee b$ leur PPCM.

Division euclidienne, b entier naturel non nul

$$a = bq + r, \quad 0 \leq r < b$$

Congruence

$$a \equiv b\,[n] \Leftrightarrow n \mid a - b$$

Bézout

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

Gauss

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

Fermat, p premier ne divisant pas a

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

Fermat, p premier, tout entier a

$$a^{p} \equiv a\,[p]$$

Inverse modulo n

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

Solutions de ax + by = c, a et b premiers entre eux

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

PGCD et PPCM, a et b entiers naturels non nuls

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

> **À retenir : La chaîne à reconnaître**
>
> Un premier p, puis $p \nmid a$, puis $a \wedge p = 1$, puis Fermat, puis une congruence modulo p, puis la conclusion. Chaque maillon se justifie par un énoncé que tu nommes.

Divisibilité et congruences

En clair : $a \mid b$ veut dire que $b = ka$ pour un certain entier relatif k. Par exemple $9 \mid -63$, car $-63 = (-7) \times 9$. En revanche $9 \nmid 48$.

> **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 $a = -b$.

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.

Exemple : Diviser un entier négatif

On divise -38 par 9 : $-38 = 9 \times (-5) + 7$, avec $0 \leq 7 < 9$. Le quotient vaut -5 et le reste vaut 7.

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 ».

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 $\{0, 1, \ldots, n-1\}$.

Exemple : Un reste sans gros calcul

Cherchons le reste de $53 \times 71 + 46$ modulo 8. On a $53 \equiv 5\ [8]$, $71 \equiv 7\ [8]$ et $46 \equiv 6\ [8]$. Donc

$$53 \times 71 + 46 \equiv 5 \times 7 + 6\ [8].$$

Or $5 \times 7 + 6 = 41$ et $41 \equiv 1\ [8]$. Le reste est 1.

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.

Méthode : Reste d'une puissance

1. Repère un petit exposant $k \geq 1$ pour lequel $a^k \equiv 1\ [n]$.
2. Divise l'exposant N par k : $N = kq + r$, avec $0 \leq r < k$.
3. Rédige : $a^N = (a^k)^q \times a^r$, donc $a^N \equiv a^r\ [n]$, d'après les opérations sur les congruences.

Exemple : Puissance de 3 modulo 11

$3^5 = 243 = 22 \times 11 + 1$, donc $3^5 \equiv 1\ [11]$. Comme $2026 = 5 \times 405 + 1$, on obtient

$$\begin{aligned} 3^{2026} &= (3^5)^{405} \times 3 \\ &\equiv 3\ [11]. \end{aligned}$$

Nombres premiers et décomposition

En clair : un nombre premier p vérifie $p \geq 2$ et n'a que deux diviseurs positifs, 1 et p. Leur ensemble se note $\mathbb{P}$. Le nombre 1 n'est pas premier.

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.

Exemple : 223 est-il premier ?

On a $14^2 = 196 \leq 223 < 225 = 15^2$. Il suffit donc de tester $2, 3, 5, 7, 11$ et 13. Aucun d'eux ne divise 223 : 223 est premier.

Théorème : Infinité des nombres premiers

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

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.

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

   $$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$$

   et

   $$a \vee b = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)}.$$
3. Pour tous entiers naturels non nuls a et b : $(a \wedge b)(a \vee b) = ab$.

Exemple : Lire une décomposition

$540 = 2^2 \times 3^3 \times 5$ possède $(2+1)(3+1)(1+1) = 24$ diviseurs positifs. Avec $252 = 2^2 \times 3^2 \times 7$, on lit $540 \wedge 252 = 2^2 \times 3^2 = 36$ et $540 \vee 252 = 2^2 \times 3^3 \times 5 \times 7 = 3780$.

PGCD, Euclide, Bézout, Gauss

En clair : $a \wedge b$ est le plus grand diviseur positif commun à a et b. $a \vee b$ est leur plus petit multiple commun strictement positif. Deux entiers sont **premiers entre eux** lorsque $a \wedge b = 1$.

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.

Exemple : Euclide sur 611 et 247

Division	Reste
$611 = 247 \times 2 + 117$	117
$247 = 117 \times 2 + 13$	13
$117 = 13 \times 9 + 0$	0

Le dernier reste non nul est 13, donc $611 \wedge 247 = 13$.

Méthode : Remonter Euclide pour un couple (u, v)

Isole chaque reste, puis remonte les lignes depuis le dernier reste non nul. Ici $13 = 247 - 2 \times 117$ et $117 = 611 - 2 \times 247$. On remplace :

$$13 = 611 \times (-2) + 247 \times 5.$$

Contrôle toujours ton couple en recalculant $au + bv$.

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.

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

$$au + bv = 1.$$

En pratique : pour prouver $a \wedge b = 1$, il suffit d'exhiber un couple. Par exemple $8 \times (-4) + 11 \times 3 = 1$, donc $8 \wedge 11 = 1$.

Théorème : Théorème de Gauss

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

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.

Méthode : Rédiger un argument de Gauss

1. Écris la divisibilité d'un produit : $a \mid bc$.
2. Justifie $a \wedge b = 1$: par un couple de Bézout, par les décompositions, ou parce que a est premier et $a \nmid b$.
3. Conclus en nommant le théorème. Exemple : $15 \mid 4m$ et $15 \wedge 4 = 1$, donc $15 \mid m$ d'après le théorème de Gauss.

$\mathbb{Z}$/n$\mathbb{Z}$ et petit théorème de Fermat

En clair : modulo $n \geq 2$, la classe $\overline{a}$ réunit tous les entiers qui ont le même reste que a. Il y a exactement n classes : $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. On calcule sur les classes comme sur les restes : $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{ab}$.

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 $a \wedge n = 1$.

Méthode : Inverser une classe

Vérifie $a \wedge n = 1$, trouve u et v tels que $au + nv = 1$, puis conclus : $\overline{a} \times \overline{u} = \overline{1}$. Modulo 26 : $7 \times (-11) + 26 \times 3 = 1$, donc l'inverse de $\overline{7}$ est $\overline{-11} = \overline{15}$.

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 $\overline{b} = \overline{0}$.

Exemple : Les inverses dans $\mathbb{Z}$/11$\mathbb{Z}$

11 est premier : chaque classe non nulle a un inverse.

$\overline{a}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
inverse	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{3}$	$\overline{9}$	$\overline{2}$	$\overline{8}$	$\overline{7}$	$\overline{5}$	$\overline{10}$

Le petit théorème de Fermat est utilisé dans 11 des 13 exercices d'arithmétique consultés.

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 : $a^p \equiv a\ [p]$.

Méthode : Fermat puis réduction de l'exposant modulo p – 1

1. Écris les deux hypothèses : p est premier et $p \nmid a$.
2. Déduis-en $a^{p-1} \equiv 1\ [p]$.
3. Divise l'exposant N par $p-1$: $N = (p-1)q + r$, avec $0 \leq r < p-1$.
4. Conclus : $a^N \equiv a^r\ [p]$.

Exemple : Reste de 6 puissance 1000 modulo 17

17 est premier et $17 \nmid 6$, donc $6^{16} \equiv 1\ [17]$. Or $1000 = 16 \times 62 + 8$, donc

$$6^{1000} \equiv 6^8\ [17].$$

Puis $6^2 = 36 \equiv 2\ [17]$, d'où $6^8 \equiv 2^4 = 16\ [17]$. Le reste de 6^{1000} dans la division par 17 est 16.

Équation ax + by = c

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 $d \mid c$.

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

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

Méthode : Résoudre ax + by = c : Bézout puis Gauss

1. Calcule $d = a \wedge b$. Si $d \nmid c$, il n'y a aucune solution.
2. Sinon, divise l'équation par d : les nouveaux coefficients sont premiers entre eux.
3. Trouve une solution particulière (x_0, y_0), par exemple à partir d'un couple de Bézout.
4. Écris toutes les solutions avec les coefficients simplifiés, puis vérifie-les dans l'équation.

Exemple : Résoudre 18x + 42y = 30

Ici $d = 18 \wedge 42 = 6$ et $6 \mid 30$. On simplifie : $3x + 7y = 5$, avec $3 \wedge 7 = 1$. Comme $3 \times (-2) + 7 \times 1 = 1$, le couple $(-10, 5)$ est solution. Les solutions sont les couples

$$(-10 + 7k,\ 5 - 3k), \quad k \in \mathbb{Z}.$$

En revanche, $18x + 42y = 25$ n'a aucune solution, car $6 \nmid 25$.

Écriture en base b

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 $n = \overline{a_k a_{k-1} \ldots a_1 a_0}^{(b)}$.

Exemple : 2026 en base 7

Division par 7	Reste
$2026 = 7 \times 289 + 3$	3
$289 = 7 \times 41 + 2$	2
$41 = 7 \times 5 + 6$	6
$5 = 7 \times 0 + 5$	5

On lit les restes du dernier au premier : $2026 = \overline{5623}^{(7)}$.

Exemple : Retour en base dix

On développe selon les puissances de la base : $\overline{10110}^{(2)} = 2^4 + 2^2 + 2 = 22$. Chaque chiffre en base b reste compris entre 0 et $b - 1$.

Méthodes d'examen

Tu dois	Outil	À écrire d'abord
trouver le reste d'une puissance	cycle des restes ou Fermat	le module ; pour Fermat, p premier et $p \nmid a$
montrer $a \wedge b = 1$	Bézout	un couple (u, v) et le calcul $au + bv = 1$
passer de $a \mid bc$ à $a \mid c$	Gauss	$a \wedge b = 1$
inverser $\overline{a}$ modulo n	Bézout	$a \wedge n = 1$
résoudre $ax + by = c$	Bézout puis Gauss	$d \mid c$ et une solution particulière
décider si n est premier	premiers p tels que $p^2 \leq n$	la liste des premiers testés

Méthode : La chaîne « un premier p »

1. **Un premier** : introduis p et dis pourquoi il est premier (hypothèse, ou plus petit diviseur premier d'un entier).
2. **Premiers entre eux** : montre que $p \nmid a$, puis déduis $a \wedge p = 1$.
3. **Fermat** : les deux hypothèses écrites, pose $a^{p-1} \equiv 1\ [p]$.
4. **Congruence** : combine avec la donnée de l'énoncé, module toujours écrit.
5. **Conclusion** : par exemple une division de l'exposant par $p - 1$, ou une contradiction.

Exemple : La chaîne sur un exemple

Soit p un nombre premier différent de 5. Ses seuls diviseurs positifs sont 1 et p, donc $5 \nmid p$. Comme 5 est premier, Fermat donne $p^4 \equiv 1\ [5]$. Puis $42 = 4 \times 10 + 2$, donc

$$\begin{aligned} p^{42} &= (p^4)^{10} \times p^2 \\ &\equiv p^2\ [5]. \end{aligned}$$

Méthode : Raisonner sur le plus petit diviseur premier

1. Pose p le plus petit diviseur premier de n : il existe dès que $n \geq 2$.
2. Traduis l'hypothèse de l'énoncé en congruence modulo p.
3. Exploite la minimalité : aucun entier compris entre 2 et $p - 1$ ne divise n.

Exemple : Premiers entre eux pour tout k

Pour tout entier k : $(3k+2)\times 2+(2k+1)\times(-3)=1$. D'après le théorème de Bézout, $(3k+2)\wedge(2k+1)=1$.

Point important : savoir écrire une identité $au+bv=1$, puis la vérifier par le calcul.

Pièges classiques

Attention : Simplifier une congruence

$4\times 5\equiv 4\times 2\ [12]$, et pourtant $5\not\equiv 2\ [12]$. Ici $4\wedge 12=4$. En revanche, si $cx\equiv cy\ [n]$ et $c\wedge n=1$, on peut simplifier : $n\mid c(x-y)$ et le théorème de Gauss donnent $n\mid x-y$.

Attention : Les hypothèses de Fermat

La forme $a^{p-1}\equiv 1\ [p]$ exige $p\nmid a$: avec $p=11$ et $a=22$, on a $22^{10}\equiv 0\ [11]$. Elle exige aussi un module premier : avec 9, qui n'est pas premier, $2^8=256\equiv 4\ [9]$.

Attention : Gauss sans primalité relative

$10\mid 4\times 15$, mais $10\nmid 4$ et $10\nmid 15$. Gauss exige $a\wedge b=1$, or $10\wedge 4=2$.

Attention : Lire une égalité de Bézout

$9\times 1+15\times 1=24$, et pourtant $9\wedge 15=3$. Une égalité $au+bv=k$ ne donne pas le PGCD en général : elle dit seulement que $a\wedge b$ divise k. Avec $k=1$, en revanche, on conclut $a\wedge b=1$ par le théorème de Bézout.

Attention : Un reste négatif

$-50=7\times(-7)-1$ n'est pas une division euclidienne. On écrit $-50=7\times(-8)+6$, avec $0\leq 6<7$.

Attention : Produit nul modulo n

Dans $\mathbb{Z}/10\mathbb{Z}$, $\overline{4}\times\overline{5}=\overline{0}$, alors qu'aucune des deux classes n'est nulle. Cette règle ne vaut que modulo un nombre premier.

Attention : Deux barres différentes

$\overline{12}^{(5)}$ désigne le nombre 7 écrit en base 5. Sans l'exposant, $\overline{12}$ est une classe de $\mathbb{Z}/n\mathbb{Z}$.

Checklist avant l'examen

- Chaque division euclidienne porte son encadrement $0 \leq r < b$.
- Chaque congruence porte son module.
- Avant Gauss, la primalité relative est écrite et justifiée.
- Avant Fermat, « p est premier » et « $p \nmid a$ » sont écrits.
- Chaque couple de Bézout est vérifié par le calcul.
- Les solutions de $ax + by = c$ sont remplacées dans l'équation.
- Avec Fermat, l'exposant se réduit modulo $p - 1$, jamais modulo p.