Arithmétique

Mathématiques expertes
Terminale générale

Divisiblité, division euclidienne et congruences

« La mathématique est la reine des sciences
et l'arithmétique est la reine des mathématiques »,

Carl Friedrich Gauss (1777 - 1855)

Table des matières

I - Échauffements

Exercice 1 **Divisiblité par 3 et par 9**
Les nombres suivants sont-ils divisibles par 3 ? par 9 ? par 6 ? par 18 ?
27 - 129 - 567 - 837 - 22134 - 1556 - 50166

Exercice 2 **Sur la parité**

a) Quelle est la parité du carré d'un nombre pair ? du carré d'un nombre impair ?

b) Quelle est la parité du produit de deux nombres pairs ? de deux nombres impairs ?

c) Quelle est la parité de la somme de deux nombres pairs ? de deux nombres impairs ?

d) Énoncer une règle sur la parité du produit de deux entiers et une règle sur la parité de la somme de deux entiers.

Exercice 3 **Sur les puissances**

Écrire sous la forme de produits et puissances, plus simples : $(5^2)^6$ - $(2\times 3^2)^3$ - $(2^{2n+1})^3$ - $\left(\frac{5^2}{3}\right)^4$

Factoriser : $2^{n+3}-2^n$ - $3^{2n+1}-3^{n+1}$ - $4^{n+1}-2^{n+2}$

II - Introduction - A propos de $\mathbb{N}$

L'arithmétique est la branche des mathématiques qui s'intéresse aux nombres entiers (naturels et relatifs), à leurs relations et propriétés en lien avec les opérations élémentaires : addition, soustraction, multiplication et division.
Tous les problèmes concernent donc ici l'ensemble des entiers naturels $\mathbb{N}$ ou celui des entiers relatif $\mathbb{Z}$.

Propriété ***Axiomes de*** $\mathbb{N}$

- ***Principe du bon ordre :*** *toute partie de* $\mathbb{N}$ *admet un plus petit élément*
- ***Principe de descente infinie :*** *toute suite dans* $\mathbb{N}$ *strictement décroissante est finie.*
- ***Principe des tiroirs :*** *si l'on range* $(n+1)$ *chaussettes dans* n *tiroirs, alors un tiroir contiendra au moins deux chaussettes.*

Remarques :

— Le principe de bon ordre permet de donner une démonstration du principe de récurrence (qui devient alors un théorème de récurrence), voir la démonstration là

— Le reste de la division par 7 d'un entier non multiple de 7 ne peut prendre que 6 valeurs : 1, 2, ...,6.
Ainsi, à partir de la 7ème division, on retrouve forcément un reste déjà obtenu (7 resultats dans 6 tiroirs). Par exemple, on a $\frac{10}{7}=1,42857\,42857\,42\ldots$ est le développement est périodique.

Exercice 4 Je dispose de 100 chaussettes, 50 noires et 50 rouges, toutes mélangées en vrac.
Avoir une chaussette rouge à un pied et une noire à l'autre est particulièrement moche.
Combien dois-je en tirer, au minimum, pour être sûr d'avoir une paire de chaussettes de la même couleur ?

III - Divisibilité dans $\mathbb{Z}$

Propriété *Rappels de règles de divisibilité :*

- *Un entier est divisible par 2 si et seulement si son chiffre des unités l'est, c'est-à-dire s'il se termnie par 0, 2, 4, 6 ou 8.*
  Un entier divisible par 2 est dit ***pair****. S'il ne l'est pas, il est* ***impair****.*
- *Un entier est divisible par 3 si et seulement si la somme de ses chiffres l'est*
- *Un entier est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres l'est*
- *Un entier est divisible par 5 si et seulement si son chiffre des unités l'est, c'est-à-dire s'il se termnie par 0 ou 5*
- *Un entier est divisible par 10 si et seulement si il est divisible à la fois par 2 et par 5, donc s'il se termine par 0.*
- *Un entier est divisible par 9 si et seulement si la somme de ses chiffres l'est*

Exercice 5

a) Donner les éventuels diviseurs parmi 2, 3, 4, 5, 9 10 des nombres suivants :
20 - 54 - 126 - 1932 - - 2020 - 2040 - 10 004

b) Donner tous les diviseurs de : 20 - 36 - 54 -

Exercice 6

a) Déterminer tous les couples d'entiers naturels $(x;y)$ tels que $x^2 - 2xy = 15$

b) Déterminer tous les couples d'entiers naturels $(x;y)$ tels que $4x = 20 + 2xy$

Définition *Soit a et b deux entiers relatifs.*
On dit que a divise b lorsque il existe un entier relatif k tel que $b = ka$.
On note $a|b$.
On dit aussi que a est un ***diviseur*** *de b, ou encore que b est un* ***multiple*** *de a.*

Exemples :

- $3|15$ car $15 = 5 \times 3$ donc 3 divise 15, et 15 est un multiple de 3.
- $3|-24$ car $-24 = 3 \times (-8)$ donc -8 et 3 sont des diviseurs de -24.
- Tous les diviseurs de 24 dans $\mathbb{N}$ sont 1 ; 2 ; 3 ; 4 ; 8 ; 12 ; 24

Propriété ***Divisibilité et combinaison linéraire***
Si $a|b$ et $a|c$ alors, pour tous entiers relatifs α et β,

$$a|(\alpha b + \beta c)$$

Démonstration: On revient à la définition de la divisibilité : il existe deux entiers relatifs k et l tels que

$$\begin{cases} a|b \iff b = ka \\ a|c \iff c = la \end{cases}$$

Maintenant, en multipliant par α la 1ère égalité et β la 2ème puis en les ajoutant terme à terme, on obtient

$$\alpha b + \beta c = \alpha(ka) + \beta(la) = a\underbrace{(\alpha k + \beta l)}_{K \in \mathbf{Z}}$$

ce qui montre exactement que $a|(\alpha b + \beta c)$. □

Exemples :

- $7|14$ et $7|700$ donc $7|728$ car $728 = 2 \times 14 + 1 \times 700$.

- Trouver une condition sur les diviseurs communs positifs à $b = 3k + 1$ et $c = 5k - 2$, pour un entier k quelconque.
  Si a est un tel diviseur, alors a divise toute combinaison linéaire de b et c, en particulier, a divise

$$5b - 3c = 5(3k + 1) - 3(5k - 2) = 11$$

  Or 11 est premier : ses seuls diviseurs sont 1 lui-même.
  Ainsi, un diviseur commun à $b = 3k + 1$ et $c = 5k - 2$ ne peut être que 1 ou 11.

Exercice 7 Déterminer, de deux manières différentes, les entiers relatifs n tels que $(n - 3)$ divise $(n + 5)$.

a) en revenant à la définition de la divisibilité

b) en remarquant que $(n - 3)$ divise $(n - 3)$ et en faisant intervenir une combinaison linéaire judicieuse de $(n - 3)$ et $(n + 5)$.

Exercice 8

1. Pour quelles valeurs de l'entier naturel n a-t-on $(n + 8)$ divisible par n ?
2. Pour quelles valeurs de l'entier relatif n la fraction $\dfrac{6n + 12}{2n + 1}$ est-elle un entier relatif ?

Exercice 9

a) Montrer que si un entier naturel d divise $(12n + 7)$ et $(3n + 1)$ alors il divise 3.

b) En déduire que la fraction $\dfrac{12n + 7}{3n + 1}$ est irréductible.

IV - Division euclidienne

Rappel : poser la division de 34 par 4

$$\begin{array}{r|l} 35 & 4 \\ \cline{2-2} -32 & 8 \\ 3 & \end{array}$$

ce qui signifie que $35 = 4 \times 8 + 3$.
Dans ce calcul,

- $a = 35$ est le **dividende**
- $b = 4$ est le **diviseur**
- $q = 5$ est le **quotient**
- $r = 3$ est le **reste**

Cette opération s'appelle la **division euclidienne de a par b** :

Théorème *Soit a un entier relatif et b un entier naturel non nul.*
Il existe alors un unique couple d'entiers relatifs $(q; r)$ tels que

$$a = bq + r \ , \ \textit{avec } 0 \leqslant r < b$$

Exemple : Écrire les divisions euclidiennes de 112 par 5 puis de 86 par 7.

Exercice 10 Trouver les entiers naturels n qui ont, dans la division euclidienne par 4, un quotient égal au reste.

Exercice 11 Trouver un entier naturel qui, dans la division euclidienne par 23 a pour reste 1, et dans la division euclidienne par 17 a le même quotient et pour reste 13.

Exercice 12 La différence de deux entiers naturels est 885. Si on divise l'un par l'autre, le quotient est 29 et le reste 17. Quels sont ces deux entiers ?

Exercice 13 Un entier naturel n est tel que si on le divise par 5 le reste vaut 3 et si on le divise par 6 le reste augmente de 1 et le quotient diminue de 1. Déterminer n.

Exercice 14 Soit n et p deux entiers naturels. On sait que le reste dans la division euclidienne de n par 11 vaut 8 et que le reste dans la division euclidienne de p par 11 vaut 7.

Quel est le reste de $n+p$ dans la division euclidienne par 11 ?

V - Congruences

1) Définition - Relation d'équivalence

Définition *Soit a et b deux entiers relatifs et $n \geqslant 2$ un entier naturel.*
On dit que a et b sont congrus modulo n lorsque a et b ont le même reste dans la division euclidienne par n.
On note

$$a \equiv b\,[n] \quad ou \quad a \equiv b \mod n$$

Exemples

- $47 = 9 \times 5 + 2$ et $32 = 6 \times 5 + 2$ d'où $47 \equiv 32\,[5]$
  En fait, $47 \equiv 2\,[5]$ et $32 \equiv 2\,[5]$
- $40 \equiv 0\,[2]$ car $40 = 20 \times 2 + 0$
- $-3 \equiv 4\,[7]$ car $-3 = -1 \times 7 + 4$

Corollaire
- *Tout nombre est congru à son reste dans la division euclidienne : si $a = bq + r$ alors $a \equiv r\,[q]$*
- *n est un diviseur de a si et seulement si $a \equiv 0\,[n]$ ($\iff a = qn + 0$)*
- *Un nombre a est pair si et seulement si $a \equiv 0\,[2]$*
  a est impair si et seulement si $a \equiv 1\,[2]$
- $a \equiv b\,[n] \iff a - b \equiv 0\,[n]$

Cette relation « est congru à » est ce qu'on appelle **une relation d'équivalence**. Ce type de relation est fondamentale en mathématiques : elle permet de mettre en relation des éléments dans un ensemble, donc les catégoriser suivant une propriété donnée. Plus tard (après le bac...) on pourra ainsi regarder non plus chaque élément seul, mais chaque groupe d'éléments ainsi formé, qu'on appelle alors une classe d'équivalence, et travailler plus abstraitement sur les propriétés de chaque classe.

Propriété *La congruence est une **relation d'équivalence**, c'est-à-dire une relation qui vérifie, pour tous entiers a, b et c,*

1. ***Réflexivité :*** $a \equiv a\,[n]$
2. ***Symétrie :*** $a \equiv b\,[n] \Longrightarrow b \equiv a\,[n]$
3. ***Transitivité :*** *si* $a \equiv b\,[n]$ *et* $b \equiv c\,[n]$ *alors* $a \equiv c\,[n]$

Autres exemples :

— La relation « est égale à » est une relation d'équivalence sur l'ensemble des nombres entiers (ou des nombres réels, ou des fonctions, ...)
— la relation « avoir le même âge » est une relation d'équivalence sur l'ensemble des êtres humains
— la relation « être parallèle à » est une relation d'équivalence sur l'ensemble des droites du plan

— Dans l'ensemble des couples de $\mathbb{N}^2$, on définit la relation d'équivalence (essayer de montrer que cette relation est bien réflexive, symétrique et transitive...) entre deux couples

$$(a;b) \equiv (c;d) \iff ad = bc$$

Cette relation d'équivalence s'écrit aussi $ad = bc \iff \dfrac{a}{b} = \dfrac{c}{d}$: c'est l'égalité entre les fractions !
Une fraction est bien un couple d'entiers (numérateur ; dénominateur) qui admet une infinité de représentant, par exemple $(1;3) \equiv (2;6) \equiv (12;36) \equiv \dots$
Dans notre utilisation des fractions, ensuite, on peut se contenter d'utiliser un représentant quelconque pour toute une classe d'équivalence, $(1;3)$ dans l'exemple précédent.
On utilise ainsi déjà, très couramment, des classes d'équivalence en maths !

2) Congruences et opérations

Il est important de savoir comment se comportent les opérations usuelles avec les congruences.

Propriété *Soit a, b, c et d des entiers relatifs, et $n \geqslant 2$ un entier naturel.*
Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$ alors

1. $a + c \equiv b + d\,[n]$ ***(addition terme à terme)***
2. $a - c \equiv b - d\,[n]$ ***(soustraction terme à terme)***
3. $ac \equiv bd\,[n]$ ***(multiplication terme à terme)***
   En particulier, pour tout entier p, $a^p \equiv b^p\,[n]$

Démonstration: La démonstration est assez importante à connaître car elle contient des mécanismes très courants et utiles (en exercices entre autre). L'idée principale est de revenir à la définition de la congruence et la division euclidienne.
Pour le 1er point, on traduit :

$$\begin{cases} a \equiv b\,[n] \iff a = kn + b \\ c \equiv d\,[n] \iff c = k'n + d \end{cases}$$

d'où, en ajoutant termes à termes

$$\begin{array}{rrcl} & a + c & = & (k + k')n + b + d \\ \iff & (a + c) & = & k''n + (b + d) \\ \iff & (a + c) & = & (b + d)\,[n] \end{array}$$

On obtient le deuxième point de même en soustrayant termes à termes.
De même encore, en mulipliant termes à termes, puis en développent et ordonnant, on obtient

$$\begin{array}{rcl} ac & = & (kn + b)(k'n + d) \\ & = & kk'n^2 + kdn + k'bn + bd \end{array}$$

Enfin, pour faire apparître la division euclidienne par n, on factorise au plus par n, soit

$$ac = n \underbrace{\left(kk'n + kd + k'b\right)}_{q} + bd$$

d'où

$$ac = qn + bd \iff ac = bd\,[n]$$

□

Donnons maintenant deux exemples d'utilisation de ces règles de calculs sur les congruences.

Exemple 1 : Montrer que, pour tout entier n, le produit $n(n+1)(2n+1)$ est divisible par 3.

Il n'y a que 3 restes possibles dans la division par 3, et on peut penser à traiter ce genre de problème par **disjonction de cas**, c'est-à-dire en étudiant **tous les cas**.
Par exemple, sous la forme d'un tableau de congruence :

$n\,[3]$	0	1	2
$(n+1)\,[3]$	1	2	$3\equiv 0$
$(2n+1)\,[3]$	1	$3\equiv 0$	$5\equiv 2$
$n(n+1)(2n+3)[3]$	0	0	0

Dans tous les cas, le produit est congru à 0 modulo 3, ce qui signifie exactement que ce produit est divisible par 3.

Exemple 2 : Donner le reste de la division euclidienne de 18^{23} par 7.

Méthode 1 : par congruences successives. On a $18 = 2\times 7+4$ donc $18\equiv 4\,[7]$ et donc $18^{23}\equiv 4^{23}\,[7]$
On dimminue la puissance en écrivant maintenant $4^{23} = (4^2)^{11}\times 4$
or $4^2 = 16\equiv 2\,[7]$, d'où $4^{23} = (4^2)^{11}\times 4\equiv 2^{11}\times 4\,[7]$
Maintenant $2^{11}\times 4 = 2^{11}\times 2^2 = 2^{13}$ et on cherche encore à diminuer la puissance : $2^{13} = (2^3)^4\times 2$
Mais, $2^3 = 8\equiv 1\,[7]$ d'où $2^{13}\equiv 1\times 2\,[7]$.
Finalement, par transitivité, $18^{23}\equiv 2\,[7]$

Méthode 2 : Dans la méthode précédente, dès qu'on arrive à une congruence à 1, les calculs sont grandement simplifiés. Autant chercher cela dès le début :
On a $18^1 = 2\times 7+4$ donc $18^1\equiv 4\,[7]$
Ensuite, $18^2 = 18\times 18\equiv 4\times 4\,[7]\equiv 16\,[7]\equiv 2\,[7]$
Après, $18^3 = 18\times 18^2\equiv 4\times 2\,[7]\equiv 1\,[7]$.
On va donc chercher à faire apparaître cette puissance :

$$18^{23} = \left(18^3\right)^7\times 18^2$$

et donc, avec les résultats précédents,

$$18^{23}\equiv 1^7\times 2\,[7]\equiv 2\,[7]$$

Exercice 15 Donner le reste de la division euclidienne de 4^2 par 15.
En déduire que que $4^{6n}-1$ est divisible par 15.

Exercice 16 Déterminer le reste de la division euclidienne de 39^{60} par 7.

Exercice 17 Déterminer le chiffre des unités dans l'écriture décimale de 3^{2023}.

Exercice 18

1. Déterminer, suivant les valeurs de n, les restes possibles de 2^n dans la division par 9. Résumer les résultats dans un tableau de congruence.
2. En déduire les entiers n tels que 2^n-1 est divisible par 9.

Exercice 19

1. Déterminer, suivant les valeurs de n, les restes possibles de 3^n dans la division par 7. Résumer les résultats dans un tableau de congruence.
2. En déduire les entiers n tels que 3^n-6 est divisible par 7.
3. En déduire que $164^{2021}\equiv 5[7]$.

Exercice 20 Le 1er janvier 2012 était un dimanche.

1. Calculer le nombre de jours séparant ce 1er janvier 2012 du 1er janvier 2019.
   En déduire quel était le jour de la semaine du 1er janvier 2019.
2. Quel est le jour de la semaine du 1er janvier 2040 ?

Exercice 21 On appelle inverse de x modulo 5, un entier y tel que $xy \equiv 1[5]$.

1. Déterminer un inverse modulo 5 de $x = 2$.
2. Déterminer un inverse modulo 5 de $x = 3$ et $x = 4$.
3. Est-ce que $x = 5$ admet un inverse ?
4. À l'aide d'un tableau de congruence, déterminer suivant la valeur de x son inverse modulo 5.
5. Résoudre les équations $E_1 : 2x \equiv 3[5]$ et $E_2 : 9x \equiv 1[5]$

Remarque : L'ensemble $\mathbb{F}_5 = \{0; 1; 2; 3; 4\}$ est un **corps** : tous ses éléments (sauf 0) ont un inverse dans $\mathbb{F}_5$.
Dans cet ensemble, on peut résoudre toutes les équations du premier degré $ax = b$, comme dans $\mathbb{R}$ et dans C (mais pas dans $\mathbb{N}$, et $\mathbb{Z}$).

Exercice 22 On décide de former des nombres dans le système décimal en écrivant de gauche à droite quatre chiffres consécutifs dans l'ordre croissant puis on permute les deux premiers chiffres de gauche.
Par exemple, à partir de 4567 on obtient 5467, ou encore à partir de 2345 on obtient 3245.

Démontrer que tous les entiers naturels ainsi obtenus sont multiples de 11.

Exercice 23 On considère un entier de 3 chiffres. On appelle renversé de cet entier le nombre qui s'écrit en échangeant les chiffres des centaines et des unités.
Par exemple, le renversé de 238 est 832.

Montrer que la différence entre un entier et son renversé est divisible par 9.

Exercice 24 On considère la suite (u_n) d'entiers définie par $u_0 = 14$ et, pour tout entier naturel n,

$$u_{n+1} = 5u_n - 6$$

1. Calculer u_1, u_2, u_3 et u_4.
   Quelle conjecture peut-on faire concernant les deux derniers chiffres de u_n ?
2. Montrer que, pour tout entier n, on a $u_{n+2} \equiv u_n[4]$.
   En déduire que, pour tout entier n, on a $u_{2n} \equiv 2[4]$ et $u_{2n+1} \equiv 0[4]$.
3. a) Montrer par récurrence que pour tout entier naturel n, on a $2u_n = 5^{n+2} + 3$.
   b) En déduire que, pour tout entier naturel n, $2u_n \equiv 28[100]$.
   c) Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.