Divisibilité et nombres premiers

Table des matières

I Divisibilité dans $\mathbb{Z}$: **3**

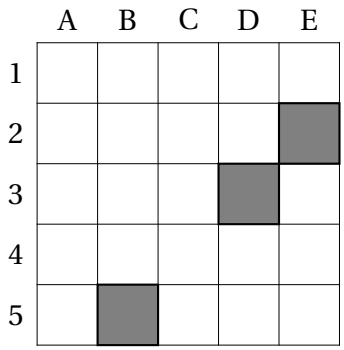
II Division euclidienne des entiers dans $\mathbb{N}$: **5**

III Congruences dans $\mathbb{Z}$: **6**

IV Critères de divisiblilité **8**

Activité d'initiation (nombres croisés) (livre spécialité (Didier)

Remplir la grille de nombres croisés ci-dessous sachant que tous les nombres y figurant sont des entiers naturels non nuls.



Horizontalement

1. Carré parfait dont le produit des chiffres est 756.
2. Le nombre formé de ses deux premiers chiffres est le même que celui formé de ses deux derniers chiffres.
3. Multiple de 139.
   Reste de la division euclidienne de 2001 par 9.
4. Permutation de 23444.
5. Carré parfait.
   Le produit de ses chiffres est 392.

Verticalement

A La somme de ses chiffres est 35.

B Entier divisible par 11.

C Nombre palindrome (qui se lit aussi bien à l'endroit qu'à l'envers).

D Nombre premier. Cube parfait.

E Entier naturel admettant un seul diviseur positif. Le produit de ses chiffres est 72 et seul son dernier chiffe est pair.

I Divisibilité dans $\mathbb{Z}$:

Rappel : On note $\mathbb{N} = \{0\,;\,1\,;\,2\,;\,3\,;\,\cdots\}$ l'ensemble des entiers naturels et $\mathbb{Z} = \{\cdots\,;\,-3\,;\,-3\,;\,-1\,;\,0\,;\,1\,;\,2\,;\,3\,;\,\cdots\}$ l'ensemble des entiers relatifs.

Définition

Soient a et b deux entiers ($a \neq 0$). On dit que a divise b si, et seulement s'il existe un entier k tel que $b = ka$. On dit aussi que a est un diviseur de b. On dit encore que b est un multiple de a.

Exemples :

7 divise 56 car $56 = 7 \times 8$ avec 8 entier
7 est un diviseur de 56 et 56 est un multiple de 7. On peut écrire $7|56$

Remarques :

- 0 est multiple de tout entier.
- Tout entier non nul n a (au moins) pour diviseurs 1, n, -1 et $-n$.
- 1 a seulement deux diviseurs dans $\mathbb{Z}$, -1 et lui-même (donc 1 a pour seul diviseur 1 dans $\mathbb{N}$).

Remarque :

Comme a et $-a$ ont les mêmes diviseurs dans $\mathbb{Z}$, on se restreint à l'étude de la divisibilité dans $\mathbb{N}$.

Propriétés

1. Tout diviseur positif d'un naturel non nul n vérifie : $1 \leq d \leq n$.
2. Tout naturel non nul a un nombre fini de diviseurs.

Démonstrations :

Soit n un naturel non nul. L'entier d divise n s'il existe un entier k tel que $n = kd$. Si $d > 0$, alors $k > 0$ (car n est positif) et ainsi $k \geq 1$.
Par conséquent : $kd \geqslant d \Leftrightarrow n \geq d$.
L'entier n a au plus n diviseurs dans $\mathbb{N}$.
Le nombre maximum de diviseurs dans $\mathbb{Z}$ est donc $2n$.
n admet un nombre fini de diviseurs.

Remarque : 0 a une infinité de diviseurs.

Exemple : Les diviseurs de 24 dans $\mathbb{N}$ sont : $\mathscr{D}(24) = 1;2;3;4;6;12;24$
Les diviseurs de 24 dans $\mathbb{Z}$ sont : $-24;-12;6;-4;-3;-2;-1;1;2;3;4;6;12;24$

Définition :

Deux entiers relatifs sont premiers entre eux si, et seulement, leurs seuls diviseurs communs sont -1 et 1.

Exemple :

15 et 14 sont premiers entre eux : $\mathscr{D}(15) = \{-15\,;\,-5\,;\,-3\,;\,-1\,;\,1\,;\,3\,;\,5\,;\,15\}$ et $\mathscr{D}(14) = \{-14\,;\,-7\,;\,-2\,;\,-1\,;\,1\,;\,2\,;\,7\,;\,14\}$.

Propriétés

1. 1 divise a pour tout entier relatif a.
2. a divise a pour tout entier relatif a.
3. Si a divise bn et si b divise c, alors, a divise c : on dit que la relation de divisibilité est **transitive**.
   Énoncé équivalent : Si b est un multiple de a et si c est un multiple de b, alors c est un multiple de a.
4. Si a divise b et si m est un entier, alors a divise mb.
5. Si a divise b et si a divise c, alors a divise $b+c$ et plus généralement, a divise $mb+nc$ où m et n sont des entiers quelconques. ($mb+nc$ est une combinaison linéaire de b et c).

Démonstrations :

1. $a = a \times 1$, donc 1 divise a.
2. $a = a \times 1$, donc a divise a.
3. Si a divise b, alors il existe k entier tel que $b = ka$.
   Si b divise c, alors il existe k' entier tel que $c = k'b$.
   Alors $c = k'b = k'(ka) = (k'k)a$. $k'k$ est un entier, donc a divise c.
4. démonstration analogue.

Exercices d'application :

Exemple 1 : Déterminer les entiers n tels que 7 divise $n+3$.
Solution : 7 divise $n+3$ si, et seulement si, il existe un entier k tel que $n+3 = 7k$, soit $n = 7k+3$.
L'ensemble des solutions est : $\mathscr{S} = \{7k-3,\ k \in \mathbb{Z}\}$

Exemple 2 : Déterminer les entiers n tels que $2n-5$ divise 6.
Solution : Les diviseurs de 6 sont -6, -3, -2, -1, 1, 2, 3 et 6.
On résout les différentes équations et on trouve comme solutions : $\mathscr{S} = \{1\ ;\ 2\ ;\ 3\ ;\ 4\}$.

Exemple 3 : Trouver les entiers n pour lesquels $\dfrac{n+15}{n+2}$ est entier.
Solution : $n+15 = n+2+13$ donc $\dfrac{n+15}{n+2} = \dfrac{(n+2)+13}{n+2} = 1 + \dfrac{13}{n+2}$.
C'est un nombre entier si, et seulement si, $\dfrac{13}{n+2}$ est un entier, c'est-à-dire si, et seulement si $n+2$ est un diviseur de 13.
Les diviseurs de 13 sont -13, -1, 1 et 13.
On résout les quare équations : $\mathscr{S} = \{-15\ ;\ -3\ ;\ -1\ ;\ 11\}$

Exemple 4 : Déterminer les entiers n tels que 2n-3 divise n+5.
Méthode : Pour résoudre un problème du type $f(n)|g(n)$, on se ramène à $h(n)|A$.
Soit n un entier tel que $2n-3$ divise $n+5$. Alors $(2n-3)$ divise $2n+10$. Comme $2n-3$ divise $2n-3$, $2n-3$ divise $(2n+10)-(2n-3)$, c'est-à dire 13. Les diviseurs de 13 sont -13, -1, 1 et 13. On en déduit que n vaut -5, 1, 2 ou 8.

Réciproquement, ces nombres sont solutions.
Les solutions sont -5, 1, 2 ou 8.

Exemple 5 : (Équations diophantiennes : (Diophante : mathématicien, IIIe siècle après J.C.))
Déterminer les entiers x et y tels que $x^2 - y^2 = 9$.
Méthode : On essaye de se ramener à une équation du type $A \times B = C$, où on connaît les diviseurs de C.
Solution :
Remarque : si $(x\ ;\ y)$ est solutions, alors $(x\ ;\ -y)$, $(-x\ ;\ y)$ et $(-x\ ;\ -y)$ sont aussi solutions. On peut alors se restreindre à x et y naturels.
$x^2 - y^2 = (x-y)(x+y)$.
Ainsi, $x - y$ et $x + y$ sont des diviseurs de 9.
L'ensemble des diviseurs de 9 sont -9, -3, -1, 1, 3, 9.
Comme $x^2 - y^2$ est positif, avec x et y positifs, alors $x > y$, donc $x - y$ et $x + y$ sont positifs, et $x - y \leq x + y$.
Premier cas : $x - y = 1$. Alors $x + y = 9$, d'où $x = 5$ et $y = 4$.
Deuxième cas : $x - y = 3$. Alors $x = y = 3$ d'où $x = 3$ et $y = 0$.
Finalement, il y a six couples solutions : $(5;4)$, $(5;-4)$, $(-5;4)$, $(-5;-4)$, $(3;0)$ et $(-3;0)$.

II Division euclidienne des entiers dans $\mathbb{N}$:

On étudie de façon approfondie la division des nombres entiers vue dans les petites classes.

Théorème de la division euclidienne dans $\mathbb{N}$:
Soit a un entier et soit b un entier naturel non nul. Il existe un **unique** entier q et un unique entier r tels que $a = bq = r$, avec $0 \leqslant r < b$.

Démonstration
On admet d'abord la propriété suivante : toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Il y a deux paties à démontrer dans ce théorème : **l'existence** du couple $(q\ ;\ r)$, puis son **unicité**.

1. **Existence de q et r :**

   - Premier cas : Si $0 \leqslant a < b$, le couple $(q\ ;\ r) = (0\ ;\ a)$ convient.
   - Second cas : on suppose que $a = b$; le couple $(1\ ;\ a)$ convient.
   - Troisième cas : on suppose a>b (a et b sont donc tous deux strictement positifs)
     On note M l'ensemble des multiples de b strictement supérieurs à a : $M = \{kb, kb > a\}$.
     $2ba \in M$ car $2b \geqslant 1$ donc M est non vide.
     M admet donc un plus petit élément que l'on note $q + 1$.
     Par définition de q, on a donc $qb \leqslant a < (q+1)b$.

     Comme $b \leqslant a$, $b \leqslant a < q+1)b$ donc $1 < q + 1$.
     On en déduit que $q > 0$ et que q est un entier naturel.
     Posons alors $r = a - bq$. r est un entier puisque a, b et q le sont.
     $qb \leqslant a \Rightarrow r \geqslant 0$ donc r est un entier naturel.
     Comme $a < (q+1)b$, on a $0 \leqslant r < b$.

Conclusion : dans tous les cas, il existe un couple $(q\ ;\ r)$ vérifiant $a = bq + r$.

2. **Unicité de q et r :**
   Supposons qu'il existe deux couples $(q\ ;\ r)$ et $(q'\ ;\ r')$ tels que $a = bq + r$ et $a = bq' + r'$, avec $0 < r < b$ et $0 < r' < b$.
   - $a = bq + r = bq' + r'$ donc $b(q - q') = r - r'$ avec $q - q'$ entier : $r - r'$ est alors un multiple de b.
   - $0 \leqslant r < b$ donne $-b < -r \leqslant 0$.
     Or, $0 \leqslant r' < b$ d'où, en additionnant : $-b < r' - r < b$.
     Or $r' - r$ est un multiple de b, strictment compris entre $-b$ et b : le seul possible est 0.
     Par conséquent : $r' - r = 0$ donc $r = r'$.
     En reportant dans $a = bq + r = bq' + r'$, on obtient $bq + r = bq' + r$, donc $bq = bq'$, d'où $q = q'$ car $b \neq 0$.
     Le couple $(q\ ;\ r)$ est donc unique.

Définition

On dit qu'on a effectué la division euclidienne de a par b ; q est le quotient et r le reste.

Exemples :
$123 = 37 \times 3 + 12$; 12 est le reste de la division euclidienne de 123 par 3

Propriétés

1. b divise a si, et seulement si, le reste de la division de a par b est nul.
2. On peut étendre le théorème au cas où a est entier (relatif) et b entier non nul : $a = bq + r$, avec $0 \leq r < |b|$.

Exercice : Montrer que tout entier n non divisible par 5 a un carré de la forme $5p + 1$ ou $5p - 1$ (raisonner par disjonction des cas)

Exercices page 23

III Congruences dans $\mathbb{Z}$:

Définition

Soit n un entier naturel non nul. on dit que a et b sont congrus modulo n si, et seulement si, a et b ont même reste dans la division euclidienne par n.
On dit aussi que a est congru b modulo n.
Notation : $a \equiv b(n)$ ou $a \equiv b$ (modulo n) ou $a \equiv b[n]$.

Remarque : $a \equiv r[n]$ avec $0 \leq r < n$ si, et seulement si r est le reste de la division euclidienne de a par n.

Exemples : $25 \equiv 14[11]$; $25 \equiv 3[11]$.

Théorème :

Soient a et b deux entiers relatifs et n un entier naturel. a et b ont même reste dans la division euclidienne par n si, et seulement si $a-b$ est divisible par n.

Démonstration :

• Supposons que a et b aient même reste dans la division par n. il existe q et q' tels que : $a = nq + r$ et $b = nq' = r$ avec q et q' entiers et $0 \leq r < n$.
Alors : $a - b = n(q - q')$ avec $q - q'$ entier, donc $a - b$ est divisible par n.

• **Réciproque :** Supposons que $a - b$ soit divisible par n. Alors $a - b = kn$ avec k entier.
Soit r le reste de la division euclidienne de b par n. On a : $b = nq = r$, avec q entier et $0 \leq r < n$.
Alors : $a = b + kn = nq + r + kn = (k+q)n + r$ avec $0 \leq r < n$ d'où le résultat.

Corollaire :

a et b sont congrus modulo n si, et seulement si $a - b$ est divisible par n.

Propriétés

1. a est divisible par $n \Leftrightarrow a \equiv 0[n]$.
2. $n \equiv 0[n]$
3. $a \equiv a[n]$ (la relation de congruence est réflexive)
4. Si $a \equiv b[n]$ et si $b \equiv c[n]$, alors $a \equiv c[n]$ (on dit que la relation de congruence est transitive).
5. Si $a \equiv b\ [b]$, alors $b \equiv a\ [n]$ (la relation de congruence est symétrique)
6. Si $a \equiv a'[n]$ et si $b \equiv b'[n]$, alors $a + a' \equiv b + b'[n]$.
7. Si $a \equiv a'[n]$ et si $b \equiv b'[n]$, alors $aa' \equiv bb'[n]$.
8. Si $a \equiv b[n]$ et si p appartient $\mathbb{N}$, alors $a^p \equiv b^p[n]$.

Démonstration :

1. évident d'après le corollaire précédent.
2. n a pour reste 0 dans la division par n, donc $n \equiv 0[n]$.
3. $n|(a-a)$ donc $a \equiv a\ [n]$
4. Si a et b ont même reste dans la division euclidienne par n et si b et c aussi, alors a et c ont même reste ans la division euclidienne par n.
5. Si $a \equiv b\ [n]$, alors $n|(a-b)$; on déduit que $n|(b-a)$ (dans $\mathbb{Z}$) et donc $b \equiv a\ [n]$
6. $a - b = qn$ et $a' - b' = q'n$. Alors $a + a' - (b + b') = (q + q')n$ donc $a + a' - (b + b')$ est divisible par n, d'où le résultat.
7. On a les mêmes hypothèses, donc $a - b = qn$ et $a' - b' = q'n$; on peut écrire $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a') = aq'n + b'qn = n(aq' + b'q)$.
   Il est clair que $aq' + b'q \in \mathbb{Z}$ (somme et produit d'entiers).
   Par conséquent : $n|(ab - a'b')$ donc $ab \equiv a'b'\ [n]$
8. se montre par récurrence.

Exercice : Déterminer l'ensemble des entiers x tels que : $x + 4 \equiv 2[8]$
$x + 4 \equiv 2[8] \Leftrightarrow x \equiv -2[8] \Leftrightarrow x \equiv 6[8]$ car -2 est congru 6 modulo 8.

Exercice : Déterminer l'ensemble des x entiers tels que $5x \equiv 3[7]$
On remplit un tableau des valeurs prises modulo [7] par $5x$ lorsque x prend les 8 valeurs des restes possibles modulo 7.

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

On en déduit que les solutions sont les nombres x congrus à 2 modulo 7.

$\boxed{\mathscr{S} = \{2+7k,\ k \in \mathbb{Z}\}}$

Exercice : Déterminer le reste de la division par 7 de 2^n.
En déduire le reste de la division euclidienne de 2^{134589} par 3.

Solution :
On a : $2^0 = 1[7]$; $2^1 = 2[7]$; $2^2 = 4[7]$; $2^3 = 8 \equiv 1[7]$. On remarque que l'on va avoir un cycle modulo 3.
• Si $n \equiv 0[3]$, alors $n = 3p$ d'où $2^n = 2^{3p} = (2^3)^p \equiv 1^p[7] \equiv 1[7]$.
• Si $n \equiv 1[7]$, alors $n = 3p+1$ d'où $2^n = 2^{3p+1} = 2^{3p} \times 2 \equiv 2[7]$
• Si $n \equiv 2[7]$, alors $n = 3p+2$ d'où $2^n = 2^{3p+2} = 2^{3p} \times 4 \equiv 4[7]$
• on a : $13459 \equiv 1[3]$; par conséquent : $2^{13458} \equiv 2[7]$

IV Critères de divisiblilité

Un critère de divisibilité par n où $n \in \mathbb{N}$ ($n \geqslant 2$) est un moyen de savoir « rapidement » si un nombre est divisible par n.
Un certain nombre de critères de divisibilité ont été vus dans les petites classes, souvent sans justification.
Donnons-les et justifions-les !

Divisibilité par 2 :
Un nombre est divisible par 2 si, et seulement si, son chiffre des unités est lui-même divisible par 2.

Démonstration
Si $n < 10$, c'est évident.
Soit $n \geqslant 10$. il existe un couple unique $(q\ ;\ r)$ tel que $n = 10q + r$ avec $0 \leqslant r < 10$.
Si 2 divise n, comme 2 divise 10, 2 divise $n - 10q = r$ donc d divise r.
Réciproquement : si 2 divise r, comme 2 divise 10, 2 divise n

Divisibilité par 5 :
Un nombre est divisible par 5 si, et seulement si, son chiffre des unités est lui-même divisible par 5.

Même type de démonstration.

Divisibilité par 4 :

Un nombre A est divisible par 4 si, et seulement si, le nombre formé par le chiffre des dizaines et celui des unités est lui-même divisible par 4.

Démonstration : on effectue la division euclidienne de A par 100 : $A = 100q + r$ et on procède comme pour la divisibilité par 2 ou 5.

Divisibilité par 3 :

Un nombre A est divisible par 3 si son chiffre des unités est lui-même divisible par 3.

Démonstration : Supposons $A \geqslant 10$ (sinon, c'est évident !).
$A = \overline{a_n a_{n-1} \cdots a_k \cdots a_1 a_0}$ en écriture décimale ; par conséquent :
$A = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_k \times 10^k + \cdots + a_1 \times 10 + a_0 = \sum_{i=0}^{i=n} a_i \times 10^i$.
Raisonnons modulo 3 : on a : $10 \equiv 1\ [3]$.
Pour tout n, $10^n \equiv 1^n\ [3] \equiv 1\ [3]$.
Alors : $A \equiv a_n + a_{n-1} + \cdots + a_0 = \sum_{i=0}^{n} a_i\ [3]$ d'où le résultat.

Divisibilité par 9 :

Un nombre A est divisible par 9 si son chiffre des unités est lui-même divisible par 9.

Même démonstration, car $10 \equiv 1\ [9]$

Divisibilité par 11 :

Un nombre A est divisible par 11 si la somme alternée de ses chiffres est elle-même divisible par 11.
Si $A = \overline{a_n a_{n-1} \cdots a_k \cdots a_1 a_0}$ en notation décimale, la somme alternée des chiffres est
$a_0 - a_1 + a_2 + \cdots + (-1)^k 10^k + \cdots + \cdots + (-1)^n 10^n$.

Démonstration :
Pour tout $k \in \mathbb{N}$, $10 \equiv -1\ \ [11]$.
On en déduit : $A \equiv a_0 \times (-1)^0 + a_1 \times (-1)^1 + a_k \times \cdots + (-1)^k + a_n \times \cdots + (-1)^n\ [11] \equiv a_0 - a_1 \cdots$

Nous avons vu les principaux critères (les plus faciles). Rien n'empêche d'en trouver d'autres.

Exemple : divisibilité par 7.
Regardons les restes successifs dans la division euclidienne par 7 des puissances successives de 10.

10^k	1	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8
Reste de la division de 10^k par 7	1	3	2	6	4	5	1	3	2

On remarque un cycle (**à justifier**), donc il est facile de déterminer tous les restes de 10^n modulo 7.
Dans l'écriture décimale avec les puissances de 10, on remplace chaque puissance de 10 par son reste modulo 7.
Exemple : $689243157 = 6 \times 10^8 + 8 \times 10^7 + 9 \times 10^6 + 2 \times 10^5 + 4 \times 10^4 + 3 \times 10^3 + 1 \times 10^2 + 5 \times 10 + 7 \equiv (6 \times 2) + (9 \times 3) + (8 \times 1) + (2 \times 5) + (4 \times 4) + (3 \times 6) + (1 \times 2) + (5 \times 3) + 7\ [7] \equiv 115\ [7] \equiv 3\ [7]$.
Ce nombre n'est donc pas divisible par 7.

Autre critère de divisibilité par 7 : Soit n un nombre d'au moins trois chiffres et dont l'écriture décimale est $\overline{a_n a_{n-1} \cdots a_{k1} a_0}$.
On note d le nombre dont l'écriture décimale est $= \overline{a_n a_{n-1} \cdots a_k \cdots a_1}$ (nombre formé à partir de N en supprimant son chiffre des unités).
On pose $n_1 = d - 2a_0$.

1. Que vaut $n - 10n_1$?
2. Montrons que n est divisible par 7 si, et seulement si n_1 est divisible par 7.
3. Montrer que $n_1 < n$.
4. Si n_1 a au moins trois chiffres, on itère le procédé ; on définit ainsi une suite de nombres n_k.
   À quelle condition sur n_k n est-il divisible par 7 ?
5. Le nombre 881909 est-il divisible par 7 ?

Démonstration : On a $n = 10d + a_0$ donc $n - 10n_1 = 10d + a_0 - 10(d - 2a_0) = 21a_0$.
Supposons que $n \equiv 0$ [7] ; on a $n - 10n_1 \equiv 21a_0$ [7] $\equiv 0$ [7] donc $10n_1 \equiv 0$ [7].
Résolvons l'équation $10x \equiv 0$ [7]. Pour cela, on renseigne un tableau.
$10 \equiv 3$ [7] et soit r le reste de la division euclidienne de x par 7. Alors $10x \equiv 3r$ [7].

r	0	1	2	3	4	5	6
$10x$ [7]	0	3	6	2	5	1	4

On en déduit que $10x \equiv 0$ [7] $\Leftrightarrow x \equiv 0$ [7].
Par conséquent : $n \equiv 0$ [7] $\Rightarrow n_1 \equiv 0$ [7].
Réciproquement : si $n_1 \equiv 0$ [7], alors $n \equiv 0$ [7].

$$n - n_1 = 10d + a_0 - (d - 2a_0) = 9d + 3a_0 > 0 \text{ donc } n > n_1$$

n est divisible par 7 si, et seulement si, n_k l'est.

Pour $n = 881909$, on trouve $n_1 = 88172$, $n_2 = 8813$, $n_3 = 875$ qui est divisible par 7, donc $n = 881909$ est divisible par 7.