Chapitre 3 – Divisibilité et congruence

L'arithmétique est l'étude des entiers naturels ou relatifs et de leur rapport.
$\mathbb{N}$ est l'ensemble des **entiers naturels** : 0; 1; 2; 3; ...
$\mathbb{Z}$ est l'ensemble des **entiers relatifs** : ... ; – 2; – 1; 0; 1; 2; ...
Les bases de l'arithmétique sont les quatre opérations (addition, soustraction, multiplication et division) enseignées à l'école primaire. En Terminale, nous approfondissons ce travail avec la **relation de divisibilité**, et tout ce qu'elle permet d'étudier (congruences, PGCD, nombres premiers...).

L'histoire de l'arithmétique est très ancienne. Une tablette d'argile découverte en Mésopotamie et datée vers 1800 avant notre ère contient une liste des « triplets pythagoriciens ». En Grèce antique, Euclide (vers 300 av. JC) ou Diophante nous ont laissé des ouvrages d'arithmétique. Des mathématiciens indiens ont étudié les congruences. D'autres résultats ont été obtenus par Fermat ou Bézout aux XVI^{e} et XVII^{e} siècles. Mais c'est à partir du XIX^{e} siècle que la **théorie des nombres** prolonge les notions étudiées et au XX^{e} siècle que des applications en informatique et en cryptographie voient le jour. Le chiffrement RSA, encore utilisé à ce jour pour sécuriser des communications, repose sur les nombres premiers.

1. Divisibilité

1a. Définition

Soient $a, b \in \mathbb{Z}$. On dit que a divise b, s'il existe un entier relatif k tel que $b = ka$. On note alors $a|b$.

Remarque : les formulations suivantes sont équivalentes :
$a|b \Leftrightarrow a$ divise $b \Leftrightarrow a$ est un diviseur de $b \Leftrightarrow b$ est divisible par $a \Leftrightarrow b$ est un multiple de a

Exemple 1 : • $12 = 3 \times 4$, donc $\mathbf{3|12}$ et $\mathbf{4|12}$. Les diviseurs de 12 dans $\mathbb{N}$ sont :

• $-45 = (-5) \times 9$, donc $\mathbf{-5|-45}$ et $\mathbf{9|-45}$.

Les diviseurs de (-45) dans $\mathbb{Z}$ sont :

Cela dit, on ne s'intéresse souvent qu'aux diviseurs d'entiers naturels dans $\mathbb{N}$.

Propriétés :
- 0 est multiple de tout entier $a \in \mathbb{Z}$, car $0 = 0 \times a$. Ainsi, **pour tout $a \in \mathbb{Z}$, $a|0$.**
- 1 divise tout entier $a \in \mathbb{Z}$, car $a = 1 \times a$. Ainsi, **pour tout $a \in \mathbb{Z}$, $1|a$.**
- Si a est un multiple de b non nul, alors $|a| \geq |b|$
- Si $a|b$ **et** $b|a$, alors $a = b$ **ou** $a = -b$.

Exemple 2 : montrer que le carré d'un nombre pair est toujours un multiple de 4.

Exemple 1 Les diviseurs de 12 dans $\mathbb{N}$ sont **1 ; 2 ; 3 ; 4 ; 6 et 12**.
Les diviseurs de (-45) dans $\mathbb{Z}$ sont : **1 ; 3 ; 5 ; 9 ; 15 ; 45** et, du coup, **-1 ; -3 ; -5 ; -9 ; -15 ; -45**. *Généralement, on trouve les diviseurs par paire : la multiplication $3 \times 15 = 45$ nous permet de trouver 3 et 15 d'un coup.*
Exemple 2 Soit n un nombre pair. Il existe alors $k \in \mathbb{Z}$ tel que $n = 2k$.
Donc $n^2 = (2k)^2 = 2^2 \times k^2 = 4k^2$, ainsi **$n^2$ est multiple de 4.**

1b. Premières applications

Propriété : soient a, b et $c \in \mathbb{Z}$.
Si a divise b et c, alors a divise toute combinaison linéaire de b et c :
pour tous $m, n \in \mathbb{Z}$, a divise $(mb + nc)$

Démonstration : Si $a|b$ et $a|c$, alors il existe k et k' relatifs tels que $b = ka$ et $c = k'a$. Donc $mb + nc = mka + nk'a = a(mk + nk')$. Ainsi a divise $mb + nc$.

Propriétés *(conséquences de la propriété précédente)*

- si a divise b, alors a divise tout multiple de b — $\boldsymbol{a|b \Rightarrow}$ **pour tout** $\boldsymbol{k \in \mathbb{Z}}$, $\boldsymbol{a|kb}$
- si a divise b et a divise c, alors a divise $(b + c)$ — $\boldsymbol{(a|b \text{ et } a|c) \Rightarrow a|(b + c)}$

Exemple 1 Soit $n \in \mathbb{N}$. Montrer que $(n + 1)$ divise $(n^2 + 8n + 7)$.

Exemple 2 **a.** Déterminer tous les entiers naturels n tels que $(n - 3)$ divise $(2n + 5)$

b. Déterminer tous les nombres entiers $n > 4$ tels que $\frac{n+17}{n-4}$ soit un entier.

Exemple 1 Il s'agit de factoriser $(n^2 + 8n + 7)$ par $(n + 1)$.
D'une façon générale, pour montrer que a *divise* b, *il faut factoriser* b *par* a.

$$n^2 + 8n + 7 = n^2 + 2n + 1 + 6n + 6 = (n + 1)^2 + 6(n + 1)$$
$$= (n + 1)\big((n + 1) + 6\big) = \boldsymbol{(n + 1)(n + 7)}$$

Exemple 2 a. $(n - 3)$ divise $(2n + 5)$ s'il existe k entier tel que :

$$2n + 5 = k(n - 3)$$
$$\Leftrightarrow 2n + 5 = kn - 3k$$
$$\Leftrightarrow kn - 3k - 2n = 5$$
$$\Leftrightarrow k(n - 3) - 2n = 5$$

On cherche à factoriser le membre de gauche par $(n - 3)$.

$$\Leftrightarrow k(n - 3) - 2n + 6 = 5 + 6$$
$$\Leftrightarrow k(n - 3) - 2(n - 3) = 11$$
$$\Leftrightarrow (k - 2)(n - 3) = 11$$

11 est premier, il admet 1 ; 11 ; -1 et -11 pour diviseurs.
On peut donc avoir : • $n - 3 = 11$, soit $n = 14$ • $n - 3 = 1$, soit $n = 4$
• $n - 3 = -1$, soit $n = 2$ • $n - 3 = -11$, soit $n = -8 \notin \mathbb{N}$
Ainsi $\boldsymbol{S = \{2; 4 ; 14\}}$.

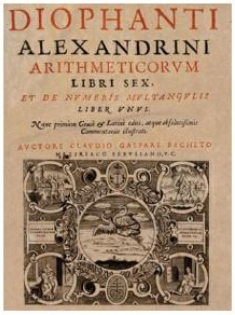
b. La fraction est un entier si $(n + 17)$ divise $(n - 4)$, c'est-à-dire s'il existe k entier tel que $n + 17 = k(n - 4)$

$$\Leftrightarrow k(n - 4) - n = 17$$
$$\Leftrightarrow k(n - 4) - n + 4 = 17 + 4$$
$$\Leftrightarrow (n - 4)(k - 1) = 21$$

21 admet 1; 3; 7 et 21 pour diviseurs. Il y a quatre possibilités :
• $n - 4 = 1$, soit $n = 5$ • $n - 4 = 3$, soit $n = 7$
• $n - 4 = 7$, soit $n = 11$ • $n - 4 = 21$, soit $n = 25$
Ainsi $\boldsymbol{S = \{5; 7; 11; 25\}}$

1c. Équations diophantiennes

Une équation diophantienne est une équation portant sur des nombres entiers.



Pour résoudre une équation diophantienne, on peut s'intéresser aux diviseurs des solutions, en **factorisant le membre de gauche et en laissant un nombre connu dans le membre de droite**.

Diophante d'Alexandrie *(II^e ou III^e s.) est un mathématicien grec connu pour son étude des équations sur les nombres rationnels, dans son ouvrage le plus connu « les Arithmétiques ». Il est surnommé le « père de l'algèbre ».*

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

b. Résoudre l'équation suivante dans $\mathbb{N}$: $x^2 = y^2 + 20$

Pierre de Fermat *(1601-1655) est un mathématicien qui a énoncé beaucoup de propriétés en arithmétique, par exemple ce qu'on a nommé plus tard le* ***grand théorème de Fermat*** *: l'équation diophantienne $x^n + y^n = z^n$ n'a pas de solution triviale pour $n \geq 2$.*
Toutefois, il ne démontrait pratiquement jamais ses énoncés, ou laissait les lecteurs le faire en guise de défi, et ce théorème n'a été démontré qu'en 1994 par Andrew Wiles.

a. $x^2 = 2xy + 15 \Leftrightarrow x^2 - 2xy = 15 \Leftrightarrow x(x - 2y) = 15$

15 admet pour diviseurs naturels 1; 3; 5 et 15.

De plus, dans les entiers naturels, on a $x > x - 2y$.

Il y a donc deux possibilités :

- $\begin{cases} x = 15 \\ x - 2y = 1 \end{cases} \Leftrightarrow \begin{cases} x = 15 \\ y = 7 \end{cases}$
- $\begin{cases} x = 5 \\ x - 2y = 3 \end{cases} \Leftrightarrow \begin{cases} x = 5 \\ y = 1 \end{cases}$

Ainsi, $\boldsymbol{S = \{(15; 7); (5; 1)\}}$

b. $x^2 = y^2 + 20 \Leftrightarrow x^2 - y^2 = 20 \Leftrightarrow (x + y)(x - y) = 20$

20 admet pour diviseurs naturels 1; 2; 4; 5; 10 et 20.

De plus, dans les entiers naturels, on a $x + y > x - y$.

Il y a donc trois possibilités :

- $\begin{cases} x + y = 20 \\ x - y = 1 \end{cases} \Leftrightarrow \begin{cases} x = 20 - y \\ (20 - y) - y = 1 \end{cases} \Leftrightarrow \begin{cases} x = 20 - y \\ -2y = -19 \end{cases} \Leftrightarrow \begin{cases} x = 10{,}5 \\ y = 9{,}5 \end{cases}$
- $\begin{cases} x + y = 10 \\ x - y = 2 \end{cases} \Leftrightarrow \begin{cases} x = 10 - y \\ (10 - y) - y = 2 \end{cases} \Leftrightarrow \begin{cases} x = 10 - y \\ -2y = -8 \end{cases} \Leftrightarrow \begin{cases} x = 6 \\ y = 4 \end{cases}$
- $\begin{cases} x + y = 5 \\ x - y = 4 \end{cases} \Leftrightarrow \begin{cases} x = 5 - y \\ (5 - y) - y = 4 \end{cases} \Leftrightarrow \begin{cases} x = 5 - y \\ -2y = -1 \end{cases} \Leftrightarrow \begin{cases} x = 4{,}5 \\ y = 0{,}5 \end{cases}$

La seule solution comportant des entiers naturels est $(\mathbf{6}; \mathbf{4})$

1d. Division euclidienne

Définition : soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ non nul. On appelle division euclidienne de a par b, l'opération qui au couple $(a; b)$ associe l'unique couple $(q; r)$ tel que $a = bq + r$ avec $0 \leq r < b$

Remarque : • a est le dividende, b est le diviseur, q est le quotient, r est le reste
• c'est la condition $0 \leq r < b$ qui assure l'unicité du couple $(q; r)$
• le nombre de restes possibles dans une division par un nombre b est fini.
Par exemple, si on divise par 4, les restes possibles sont 0 ; 1 ; 2 et 3.

Exemples

a. Donner la division euclidienne de 114 par 7. En déduire celle de (-114) par 7.
b. Trouver tous les entiers n dont le quotient dans la division par 5 donne un quotient égal à trois fois le reste.
c. Lorsqu'on divise a par b, le reste est 8 et lorsqu'on divise $2a$ par b, le reste est 5. Déterminer ce diviseur b.
d. On divise 439 par b : le quotient est 13. Quels peuvent être le diviseur et le reste r ?

a. On trouve $\mathbf{114 = 7 \times 16 + 2}$, donc $q = 16$ et $r = 2$.
On en déduit que $-114 = -7 \times 16 - 2$, mais ce n'est pas la division euclidienne car **le reste doit être positif et inférieur à 7**. Mais :

$$\begin{aligned} -114 &= -7 \times 16 - 2 \\ &= 7 \times (-16) - 2 + 7 - 7 \\ &= 7 \times (-17) + 5 \end{aligned}$$

ainsi $\boldsymbol{q = -17}$ **et** $\boldsymbol{r = 5}$.
b. La consigne se reformule ainsi : $n = 5q + r$, or $q = 3r$,
donc $n = 5 \times 3r + r = 15r + r = 16r$.
Il s'agit d'une division par 5, donc $r \in \{0; 1; 2; 3; 4\}$.
Ainsi, $\boldsymbol{S = \{0; 16; 32; 48; 64\}}$
c. On a $a = bq + 8$ et $2a = bq' + 5$, les quotients q et q' n'étant pas les mêmes.
Comme $a = bq + 8$, alors $2a = 2bq + 16$.
Donc $bq' + 5 = 2bq + 16 \Leftrightarrow bq' - 2bq = 11 \Leftrightarrow b(q' - 2q) = 11$
Les diviseurs de 11 étant 1 et 11, donc b ne peut prendre que ces deux valeurs.
Mais si b était égal à 1, le reste ne pourrait être 8 ou 5.
Donc $\boldsymbol{b = 11}$.
d. On sait que $439 = 13b + r$
Comme $\frac{439}{13} \approx 33{,}8$ on peut chercher les valeurs de b inférieures ou égales à 33 (pour avoir un reste positif).
• si $b = 33$, $439 = 13 \times 33 + 10$ et $r = 10$
• si $b = 32$, $439 = 13 \times 32 + 23$ et $r = 23$
• si $b = 31$, $439 = 13 \times 31 + 23$ et $r = 36$, or on a alors $r > b$.
Ainsi, les valeurs possibles pour $(b; r)$ sont $(\mathbf{33}; \mathbf{10})$ et $(\mathbf{32}; \mathbf{23})$.

2. Congruences

2a. Définition

Définition : soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$ non nul.
On dit que a et b sont congrus modulo n s'ils ont le même reste dans la division euclidienne par n.
On note alors $a \equiv b[n]$, mais aussi $a \equiv b(n)$ ou $a \equiv b \bmod n$

Exemples : • $23 \equiv 48[5]$, en effet, le reste de 23 et de 48 dans la division euclidienne par 5 est …
• Compléter avec des nombres de votre choix :
a. $16 \equiv \ldots \equiv \ldots \equiv \ldots \ [7]$ **b.** $101 \equiv \ldots \equiv \ldots \equiv \ldots \ [15]$
c. $8 \equiv \ldots \equiv \ldots \equiv \ldots \ [4]$ **d.** $-1 \equiv \ldots \equiv \ldots \equiv \ldots \ [6]$

Remarques : • un nombre est toujours **congru modulo n à son reste** dans la division euclidienne par n.
• a est **multiple de n** si et seulement si $a \equiv 0[n]$
• pour tout $a \in \mathbb{Z}$, $a \equiv 0[a]$.

Propriétés : Pour tout $n \in \mathbb{N}$ et pour tous $a, b, c \in \mathbb{Z}$:
• $a \equiv a[n]$ *(réflexivité)* • $a \equiv b[n] \Rightarrow b \equiv a[n]$ *(symétrie)* • $a \equiv b[n]$ et $b \equiv c[n] \Rightarrow a \equiv c[n]$ *(transitivité)*
En général, une relation entre des éléments d'un ensemble qui vérifie ces trois propriétés s'appelle une **relation d'équivalence**, ce qui signifie qu'elle fonctionne plus ou moins comme une égalité.
Ainsi, la congruence sur $\mathbb{Z}$ est une relation d'équivalence.

$23 \equiv 48[5]$ car lorsqu'on divise ces deux nombres par 5, le reste est le même : **3**.
a. $16 \equiv 2 \equiv -5 \equiv 44[7]$
b. $101 \equiv 11 \equiv -4 \equiv 56[15]$
c. $8 \equiv 0 \equiv -4 \equiv 40[4]$
d. $-1 \equiv 5 \equiv 11 \equiv -7[6]$

2b. Opérations

Propriété : soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$ non nul.

$$a \equiv b[n] \Leftrightarrow a - b \equiv 0[n]$$

Deux nombres sont congrus modulo n si leur différence est un multiple de n.

Démonstration :

$\Rightarrow$ Supposons que $a \equiv b[n]$

Il existe alors q et q' tels que $a = nq + r$ et $b = nq' + r$

Donc $a - b = (nq + r) - (nq' + r) = nq - nq' = n(q - q')$

$a - b$ est alors un multiple de n, donc $\boldsymbol{a - b \equiv 0[n]}$.

$\Leftarrow$ Supposons que $a - b \equiv 0[n]$

$a - b$ est alors multiple de n : il existe k tel que $a - b = nk$.

Ainsi, dans la division euclidienne de $a - b$ par n, le reste est 0.

Effectuons la division de a par n : $a = nq + r$. Donc

$$\begin{aligned} & a - b = nk \\ \Leftrightarrow\ & nq + r - b = kn \\ \Leftrightarrow\ & b = nq - nk + r \\ \Leftrightarrow\ & b = n(q - k) + r \end{aligned}$$

Ainsi, a et b ont le même reste r quand on les divise par n, et $\boldsymbol{a \equiv b[n]}$.

Propriétés : soient $a, b, c, d \in \mathbb{Z}$ et $n \in \mathbb{N}$ non nul.

- si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a + c \equiv b + d[n]$ et $ac \equiv bd[n]$
- si $a \equiv b[n]$ et $k \in \mathbb{N}$, alors $a^k \equiv b^k[n]$

La congruence est compatible avec l'addition, la multiplication et les puissances.

Démonstration : • si $a \equiv b[n]$ et $c \equiv d[n]$, alors $(a - b)$ et $(c - d)$ sont multiples de n d'après la propriété précédente.

Ainsi, $(a - b) + (c - d) = (a + c) - (b + d)$ est multiple de n et donc $\boldsymbol{a + c \equiv b + d[n]}$ d'après la propriété.

• si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a = qn + b$ et $c = q'n + d$.

On multiplie ces deux égalités :

$ac = (qn + b)(q'n + d)$

$= qnq'n + qnd + q'nb + bd$

$= n(qq'n + qd + q'b) + bd$

On a montré que la différence entre ac et bd est aussi un multiple de n, donc $\boldsymbol{ac \equiv bd[n]}$

• la compatibilité avec les puissances se montre facilement **par récurrence**.

Exemple 1 : $47 \equiv$ ... [9] et $58 \equiv$ ... [9] , donc $47 + 58 \equiv$ ... [9] et $47 \times 58 \equiv$ ... [9]

Exemple 2 **a.** Montrer que $16^6 \equiv 1[9]$.
b. En déduire le reste de la division euclidienne de 16^{19} par 9.

Exemple 3 À l'aide des congruences, déterminer le chiffre des unités dans l'écriture décimale de 3^{2023}.

Exemple 4 **a.** Expliquer pourquoi $25 \equiv -1[13]$.
b. En déduire que pour tout entier naturel n, $5^{4n} - 1$ est divisible par 13.

Exemple 1

$47 \equiv \mathbf{2}[9]$ et $58 \equiv \mathbf{4}[9]$, donc $47 + 58 \equiv \mathbf{6}[9]$ et $47 \times 58 \equiv \mathbf{8}[9]$.

Exemple 2

a. On sait que $16 \equiv 7[9]$, donc $16^2 \equiv 7^2 \equiv 49 \equiv 4[9]$
Puis par produit, $16^3 \equiv 16^2 \times 16 \equiv 4 \times 2 \equiv -1[9]$.
Ainsi, $16^6 \equiv (16^3)^2 \equiv (-1)^2 \equiv \mathbf{1}[\mathbf{9}]$
Dans les congruences, on adore trouver 1 !
b. $16^{19} \equiv (16^6)^3 \times 16 \equiv 1^3 \times 16 \equiv 16 \equiv 7[9]$.
Ainsi, **le reste de la division euclidienne de 16^{19} par 9 est 7.**

Exemple 3

Il s'agit de déterminer le reste de 3^{2023} dans la division par 10.
On sait que $3^4 \equiv 81 \equiv 1[10]$.
Donc $3^{2023} \equiv 3^{2020} \times 3^3 \equiv (3^4)^{505} \times 3^3 \equiv 1^{505} \times 3^3 \equiv 27 \equiv 7[10]$.
Le chiffre des unités de 3^{2023} est 7.

Exemple 4

$25 - (-1) = 26$ qui est un multiple de 13, donc $25 \equiv -1[13]$
Soit n entier naturel. $5^{4n} = (5^4)^n = ((5^2)^2)^n = (25^2)^n$
Ainsi, $5^{4n} \equiv (25^2)^n \equiv ((-1)^2)^n \equiv 1^n \equiv 1[13]$
Donc $5^{4n} - 1 \equiv 0[13]$ et **$5^{4n} - 1$ est divisible par 13**.

2c. Raisonnement par disjonction de cas

Définition : lorsque dans une démonstration, on essaie de traiter séparément différentes possibilités (par exemple, pair/impair, ou suivant la congruence d'un nombre), on fait de la disjonction de cas.

Disjonction de cas :

Exemple 1 **a.** Montrer que pour tout entier naturel n, $\frac{n(n+1)}{2}$ est un nombre entier.

b. Montrer que pour tout entier naturel n, $5n^2 + 3n$ est pair.

Séries de restes Quand on cherche la séries de restes d'une expression, on essaye de trouver un cycle qu'on représente dans un tableau. On peut ensuite faire de la disjonction de cas suivant la congruence.

Exemple 2 **a.** Déterminer les restes possibles de n^2 dans la division par 7, suivant les valeurs de l'entier n.

b. En déduire les solutions de l'équation $n^2 \equiv 2[7]$. Donner quelques exemples.

Exemple 3 **a.** Soit $n \in \mathbb{N}$. Déterminer, suivant les valeurs de n, les restes possibles de 3^n dans la division par 11.

b. En déduire les valeurs de n pour lesquelles $3^n + 7$ est un multiple de 11.

c. En déduire que $135^{2\,021} \equiv 3[11]$

Exemple 4 Pour quelles valeurs de l'entier n, le nombre $3 \times 4^n + 2$ est-il divisible par 11 ?

Exemple 1

a. Il s'agit de vérifier que $n(n+1)$ est pair pour tout entier n.

• Si n est pair, c'est le cas.

• Si n est impair, alors $(n+1)$ est pair et donc $n(n+1)$ aussi.

b. • Si n est pair, alors $5n^2$ et $3n$ sont également pairs et $5n^2 + 3n$ aussi.

• Si n est impair, alors $5n^2$ et $3n$ sont également impairs.

Leur somme $5n^2 + 3n$ est donc paire.

Exemple 2

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

Les solutions de l'équation $n^2 \equiv 2[7]$ sont donc les nombres n tels que $n \equiv 3[7]$ ou $n \equiv 4[7]$, c'est-à-dire les nombres de la forme $\mathbf{7k+3}$ ou $\mathbf{7k+4}$ avec k entier.

Exemple 3

a. On remplit le tableau en multipliant chaque case de la deuxième ligne par 3 pour obtenir la suivante.

$n \equiv \cdots [5]$	0	1	2	3	4
$3^n \equiv \cdots [11]$	1	3	9	5	4

On constate ensuite que $3^5 \equiv 1[11]$, donc les résultats suivants seront les mêmes que les 5 premiers.

b. On ajoute une ligne au tableau :

$3^n + 7 \equiv \cdots [11]$	8	10	5	1	0

Les solutions sont donc les nombres n tels que $\boldsymbol{n \equiv 4[5]}$.

c. $135 = 3 \times 45$, or $45 \equiv 1[11]$.
Ainsi, $135^{2021} \equiv 3^{2021} \times 45^{2021} \equiv 3^{2021}[11]$
et d'après la question **a**, $\boldsymbol{3^{2021} \equiv 3[11]}$.

Exemple 4

$n \equiv \cdots [5]$	0	1	2	3	4
$4^n \equiv \cdots [11]$	1	4	5	9	3
$3 \times 4^n + 2 \equiv \cdots [11]$	5	3	6	8	0

Les solutions sont donc les nombres n tels que $\boldsymbol{n \equiv 4[5]}$.

2d. Critères de divisibilité

Propriété : soit $a \in \mathbb{N}$, un nombre à m chiffres en écriture décimale.
Alors :

$$a = \sum_{k=0}^{m-1} a_k \times 10^k$$

où les nombres a_0 ; a_1 ; … ; a_{m-1} sont les chiffres de a.

Exemple : $1\,789 = 1 \times 10^3 + 7 \times 10^2 + 8 \times 10^1 + 9 \times 10^0$

Critères de divisibilité

Exemple 1
Montrer qu'un nombre est divisible par 4 ssi ses deux derniers chiffres forment un nombre divisible par 4.

Exemple 2 a. Montrer qu'un nombre est divisible par 3 ssi la somme de ses chiffres est divisible par 3.
b. Montrer qu'il en est de même pour la divisibilité par 9.
c. Étudier le critère de divisibilité par 11.

Exemple 3 a. Montrer qu'un nombre est divisible par 7 ssi le nombre de ses dizaines diminué du double du chiffre de ses unités est divisible par 7.
b. Avec ce critère, déterminer si 574 et 827 sont disivibles par 7.

Exemple 1 Soit n entier naturel.
On s'intéresse à la division euclidienne de ce nombre par 100.

$$n = 100q + r$$

où $100q$ est multiple de 4 et r correspond aux deux derniers chiffres de n. Ainsi, $n \equiv r[4]$, et n est multiple de 4 ssi ses deux derniers chiffres le sont.

Exemple 2 a. On a $10 \equiv 1[3]$ donc pour tout k entier naturel, $10^k \equiv 1[3]$.
Ainsi, pour tout nombre $n = \sum_{k=0}^{m-1} a_k \times 10^k$,
n est congru à $\sum_{k=0}^{m-1} a_k$ modulo 3, c'est-à-dire à la somme de ses chiffres.
b. De même, $10 \equiv 1[9]$.
c. Plus compliqué : $10 \equiv -1[11]$ donc $10^k \equiv (-1)^k[11]$.
Ainsi, pour tout nombre $n = \sum_{k=0}^{m-1} a_k \times 10^k$,
n est congru module 11 à la somme alternée de ses chiffres :

$$a_0 - a_1 + a_2 - a_3 + a_4 \ldots$$

et n est divisible par 11 si la somme alternée de ses chiffres l'est.

Exemple 3 a. On effectue la division de n par 10 : $n = 10q + r$,
où q est le nombre de dizaines et r le chiffre des unités.
$n \equiv 10q + r \equiv 10q + r - 7q \equiv 3q + r \equiv 3q + r - 7r \equiv 3q - 6r \equiv 3(q - 2r)[7]$
Or $3(q - 2r)$ est multiple de 7 si et seulement si $(\boldsymbol{q - 2r})$ l'est.
b. $57 - 4 \times 2 = 49$ donc 574 est divisible par 7.
$82 - 2 \times 7 = 68$ donc 827 n'est pas divisible par 7.