Divisibilité, congruences

1. Divisibilité dans $\mathbb{Z}$

Notation.
L'ensemble des entiers naturels 0, 1, 2, … se note $\mathbb{N}$.
L'ensemble des entiers relatifs …, -2, -1, 0, 1, 2, … se note $\mathbb{Z}$.

Définition. *On dit que l'entier relatif a divise l'entier relatif b lorsqu'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 que b est divisible par a.
b est alors un multiple de a.

Remarque. Tout entier relatif a avec $a \leq -2$ ou $a \geq 2$ possède au moins quatre diviseurs : 1, -1, a, $-a$. Tout entier possède un nombre fini de diviseurs, compris entre $-a$ et a.

Exemple

Soit N un entier divisible par 2 et par 3.
Il existe deux entiers k et k' tels que $N = 2k$ et $N = 3k'$. On a alors
$$N = 3N - 2N = 3 \times 2k - 2 \times 3k' = 6(k - k').$$
Cela montre que N est aussi divisible par 6.

Théorème. Soit a, b, c trois entiers relatifs. Si a divise b et b divise c, alors a divise c.

Démonstration. Il existe deux entiers k et k' tels que $b = ka$ et $c = k'b$, d'où $c = kk'a$, ce qui prouve que a divise c. ■

Exemple

3 divise 6 et 6 divise 6^7, donc 3 divise 6^7.

Théorème. Soit a, b et d trois entiers relatifs. Si d divise a et b, alors d divise toute combinaison linéaire de a et b, c'est-à-dire tout entier de la forme $au + bv$ où u et v sont des entiers.

Démonstration. Il existe deux entiers k et k' tels que $a = kd$ et $b = k'd$, d'où l'on déduit $au + bv = (ku + k'v)d$, ce qui prouve que d divise $au + bv$. ■

Exemple

3 divise 6^7 et 3 divise 21, donc 3 divise $4 \times 21 - 6^7$.

Exemple

Déterminons les entiers naturels n tels que $n + 2$ divise $3n + 1$.
Pour un tel entier n, $n + 2$ divise $n + 2$ et divise $3n + 1$, donc divise toute combinaison linéaire de ces nombres, en particulier $3(n + 2) - (3n + 1) = 5$. Réciproquement, si $n + 2$ divise 5, il divise $3(n + 2) - 5 = (3n + 1)$. Les diviseurs de 5 étant -5, -1, 1 et 5 on en déduit que $n + 2 = \pm 5$ ou $n + 2 = \pm 1$, d'où $n \in \{-7; -3; -1; 3\}$.

❖ Système décimal

Le système décimal, ou la base 10, est notre système usuel d'écriture des nombres. Dire qu'un entier s'écrit dans le système décimal sous la forme $\overline{a_n a_{n-1} \dots a_1 a_0}$ où a_n, a_{n-1}, …, a_0 sont des chiffres de 0 à 9 avec $a_n \neq 0$, c'est dire qu'il est égal à

$$a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0.$$

Exemple

$2018 = 2 \times 10^3 + 0 \times 10^2 + 1 \times 10 + 8.$

Exemple

Soit n un entier ayant 5 pour chiffre des unités. Montrer que n^2 a également 5 pour chiffre des unités.

On peut écrire $n = 10d + 5$, où d est un entier. On a alors en développant

$$n^2 = (10d + 5)^2 = 100d^2 + 100d + 25 = (100d^2 + 100d + 20) + 5 = K + 5$$

où K est un entier. Cela montre que n^2 se termine par un 5.

Exemple

Soit N un carré dont l'écriture se termine par 6. Montrons que le chiffre des dizaines de N est impair (par exemple $\mathbf{1}6 = 4^2$; $\mathbf{3}6 = 6^2$; $1\mathbf{9}6 = 14^2$; $2\mathbf{5}6 = 16^2$…)

Remarquons tout d'abord qu'un nombre ayant un chiffre des dizaines impair s'écrit $10d + u$ avec $0 \leq u \leq 9$ et où d est un entier impair.

On raisonne par disjonction de cas, en fonction du dernier chiffre de l'entier n tel que $N = n^2$.

- Supposons n est impair, c'est-à-dire se terminant par 1, 3, 5, 7 ou 9. Il existe un entier k tel que $n = 2k + 1$, donc
  $$N = n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
  ce qui montre que N est impair, son chiffre des unités ne peut donc pas être 6.
- Supposons n pair et soit u le chiffre des unités de n et d son nombre de dizaines. On a $n = 10d + u$, d'où
  $$N = n^2 = (10d + u)^2 = 100d^2 + 20du + u^2 = 10(10d^2 + 2du) + u^2.$$
  Il ne faut pas en déduire que u^2 est le chiffre des unités de N car il se peut que u^2 soit supérieur ou égal à 10. Il faut donc envisager tous cas, pour $u \in \{0; 2; 4; 6; 8\}$.
  - Si $u = 0$, alors $N = 10 \times 10d^2 + 0$ et le chiffre des unités de N est 0.
  - Si $u = 2$, alors $N = 10(10d^2 + 2d) + 4$ et le chiffre des unités de N est 4.
  - Si $u = 4$, alors
    $$N = 10(10d^2 + 8d) + 16 = 10(10d^2 + 8d + 1) + 6.$$
    Cela montre que le chiffre des unités de N est 6, et le nombre de dizaine est bien impair, puisque celui-ci est $10d^2 + 8d + 1 = 2(5d^2 + 4d) + 1$.
  - Si $u = 6$, alors
    $$N = 10(10d^2 + 12d) + 36 = 10(10d^2 + 12d + 3) + 6.$$
    Cela montre que le chiffre des unités de N est 6, et le nombre de dizaine est bien impair, puisque celui-ci est $10d^2 + 12d + 3 = 2(5d^2 + 6d + 1) + 1$.
  - Si $u = 8$, alors
    $$N = 10(10d^2 + 16d) + 64 = 10(10d^2 + 16d + 6) + 4$$
    et le chiffre des unités de N est 4.

En conclusion, on constate que le chiffre des unités de N est 6 si et seulement si le chiffre des unités de n est 4 ou 6, et dans ces cas-là, le chiffre des dizaines est impair.

2. Division euclidienne

Théorème – Définiton. Soit a et b deux entiers naturels avec b non nul.
Il existe un unique couple d'entiers naturels $(q;r)$ tels que $a = bq + r$ et $0 \leq r < b$.
On dit que a est le **dividende**, b le **diviseur**, q le **quotient** et r le **reste**.

Remarque. q est la partie entière de $\frac{a}{b}$ et r se calcule par $r = a - bq$.

Exemple

D'après l'écran de la calculatrice ci-contre, la division euclidienne de 147 par 11 s'écrit $147 = 11 \times 13 + 4$.

Démonstration.

1. **Existence de q et r.**
   Soit $E = \{m \in \mathbb{N}; mb > a\}$. Comme $b \geq 1$, on a
   $$(a+1)b \geq a + 1 > a$$
   donc E n'est pas vide. D'après l'axiome du plus petit élément (qui affirme que toute partie non vide de $\mathbb{N}$ admet un plus petit élément), il existe un entier m_0, plus petit élément de E tel que $(m_0 + 1)b \leq a < m_0 b$.
   En posant $q = m_0 - 1$ et $r = a - bq$, on a bien $a = bq + r$ et $0 \leq r < b$. En effet, comme $(m_0 - 1)b \leq a < m_0 b$, on a alors $(m_0 - 1)b - bq \leq a - bq < m_0 b - bq$, ce qui en simplifiant donne $0 \leq r < b$.

2. **Unicité de q et r.**
   Supposons qu'il existe deux couples $(q;r)$ et $(q';r')$ vérifiant la propriété. On a
   $$a = bq + r = bq' + r' \text{ avec } 0 \leq r < b \text{ et } 0 \leq r' < b.$$
   De $0 \leq r' < b$, on déduit $-b < -r' \leq 0$, d'où en ajoutant à $0 \leq r < b$ l'inégalité
   $$-b < r - r' < b.$$
   Par ailleurs $b(q - q') = r' - r$, ce qui montre que $r' - r$ est un multiple de b compris strictement entre $-b$ et b, ce peut être que 0. Ainsi $r' - r = 0$, d'où $r = r'$.
   Par suite $b(q - q') = 0$ et comme $b \neq 0$, c'est que $q - q' = 0$ et donc $q = q'$. ■

On peut étendre le résultat de la façon suivante.

Théorème. Soit a et b deux entiers avec b non nul.
Il existe un unique couple d'entiers $(q;r)$ tels que $a = bq + r$ et $0 \leq r < |b|$.

Exemple

La division euclidienne de -22 par -8 s'écrit $-22 = -8 \times 3 + 2$.

Théorème. Soit b un entier supérieur ou égal à 2. Parmi b entiers consécutifs, l'un est multiple de b.

Démonstration. Soit N le plus grand de ces entiers consécutifs. L'entier N s'écrit
$$N = bq + r \text{ avec } 0 \leq r \leq b - 1.$$

L'entier $N - r$, qui est l'un des b entiers consécutifs N, $N-1$, $N-2$, …, $N-(b-1)$ considérés s'écrit donc $N - r = bq$: c'est un multiple de b. ■

Exemple

Montrons que pour tout entier n, l'entier $N = n(n+1)(2n+1)$ est un multiple de 6.
D'après l'exemple vu dans la partie 1, il suffit de montrer qu'il est divisible par 2 et par 3.

- Parmi les deux entiers consécutifs n et $n+1$, l'un d'entre eux est un multiple de 2, il en est donc de même de N.
- Parmi les trois entiers consécutifs n, $n+1$ et $n+2$, l'un d'entre eux est un multiple de 3. Si c'est n ou $n+1$, alors N est un multiple de 3. Si c'est $n+2$, alors
$$2n + 1 = 2(n+2) - 3$$
est une combinaison linéaire de deux multiples de 3, c'est aussi un multiple de 3, ainsi que N.

Théorème. Soit b un entier supérieur ou égal à 2 et b entiers consécutifs r_0, r_1, … r_{b-1}.
Tout entier a s'écrit sous une et une seule des formes
$$bn + r_0 \; ; \; bn + r_1 \; ; \; \ldots \; ; \; bn + r_{b-1}$$
où n est un entier.

Démonstration. Parmi les b entiers consécutifs $a - r_0$, $a - r_1$, …, $a - r_{b-1}$, l'un est divisible par b, par exemple $a - r_k$ (avec $0 \leq k \leq b-1$). Il existe donc un entier relatif n tel que $a - r_k = bn$, d'où $a = bn + r_k$.
Supposons qu'il existe deux écritures distinctes de a de la forme annoncée :
$a = bn + r_k$ et $a = bn' + r_{k'}$, avec $0 \leq k, k' \leq b-1$ et n et n' deux entiers.
On a alors $b(n - n') = r_{k'} - r_k$.
Comme les entiers r_0, r_2, …, r_{b-1} sont b entiers consécutifs, on a
$$r_k = r_0 + k \text{ et } r_{k'} = r_0 + k',$$
donc $r_{k'} - r_k = k' - k$, avec $0 \leq k, k' \leq b-1$. Comme dans la preuve de l'unicité de la division euclidienne, il vient $-(b-1) \leq r_{k'} - r_k \leq b-1$, d'où $r_{k'} - r_k = 0$, puis $r_{k'} = r_k$ et enfin $n = n'$. ■

Exemple

Tout entier s'écrit $2k$ ou $2k+1$.
Tout entier s'écrit $3k$, $3k+1$ ou $3k+2$.
Tout entier s'écrit $3k-1$, $3k$ ou $3k+1$.

Exemple

Montrons que $n^2 - 1$ est divisible par 8 si et seulement si n est impair.

1. Si n est pair, alors n^2 est pair, donc $n^2 - 1$ est impair, il n'est pas divisible par 8.

2. Si n est impair, il s'écrit $n = 2k+1$ pour un certain $k \in \mathbb{Z}$. Alors
$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1).$$
Parmi les entiers consécutifs k et $k+1$ l'un des deux est pair, donc l'entier $k(k+1)$ est pair et s'écrit $2k'$ pour un certain $k' \in \mathbb{Z}$. Ainsi $n^2 - 1 = 8k'$, ce qui prouve que $n^2 - 1$ est divisible par 8.

3. Cela montre que $n^2 - 1$ est divisible par 8 si et seulement si n est impair (on dit qu'on a raisonné par disjonction de cas).

3. Congruences

Définition. *Soit m un entier naturel non nul.*
Deux entiers a et b sont dits congrus modulo m si m divise $b - a$.
On notera cela $a \equiv b \ [m]$, ou $a \equiv b \ (m)$, ou $a \equiv b \ mod\ m$.

Exemple

- $27 \equiv 19 \ [4]$ car $27 - 19 = 8 = 2 \times 4$.
- $11 \equiv -3 \ [7]$ car $11 - (-3) = 14 = 2 \times 7$.

Théorème. Soit m un entier naturel non nul.
Deux entiers a et b sont congrus modulo m si et seulement s'ils ont le même reste dans leur division euclidienne par m.

Démonstration. Supposons que a et b ait le même reste dans la division euclidienne par m. On peut écrire $a = mq + r$ et $b = mq' + r$, d'où $a - b = m(q - q')$, ce qui prouve que $a - b$ est divisible par m.
Réciproquement, si $a \equiv b \ [m]$, on a $a - b = km$ pour un certain $k \in \mathbb{Z}$, d'où $a = b + km$. La division euclidienne de b par m permet d'écrire $b = mq + r$ avec $0 \leq r < m$. Il en résulte que $a = mq + r + km = m(q + k) + r$, c'est l'écriture de la division euclidienne de a par m, le reste est bien r. ■

Remarques.

- a est un multiple de m si et seulement si $a \equiv 0 \ [m]$.
- Les nombres congrus à a modulo m sont les nombres $a + km$, $k \in \mathbb{Z}$.
- r est le reste de la division euclidienne de a par m si et seulement si $a \equiv r \ [m]$ et $0 \leq r < m$.

Théorème. Soit b un entier supérieur ou égal à 2 et b entiers consécutifs r_0, r_1, … r_{b-1}.
Tout entier a est congru modulo b à un et un seul des entiers r_0, r_1, … r_{b-1}.

Exemple

Un entier n vérifie une et une seule des égalités suivantes :
$n \equiv -2 \ [5]$; $n \equiv -1 \ [5]$; $n \equiv 0 \ [5]$; $n \equiv 1 \ [5]$; $n \equiv 2 \ [5]$.

Théorème (Transitivité). Soit a, b, c, m quatre entiers ($m \geq 0$).
Si $a \equiv b \ [m]$ et $b \equiv c \ [m]$, alors $a \equiv c \ [m]$.

Démonstration. Il existe k et k' des entiers tels que $a - b = km$ et $b - c = k'm$, on en déduit $a - c = (a - b) + (b - c) = km + k'm = (k + k')m$, ce qui prouve que $a - c$ est divisible par m, c'est-à-dire $a \equiv c \ [m]$. ■

Théorème (Compatibilité des congruences avec l'addition et la multiplication). Soit a, b, c, d, m cinq entiers ($m \geq 0$). Si $a \equiv b \ [m]$ et $c \equiv d \ [m]$, alors

- $a + c \equiv b + d \ [m]$;
- $ac \equiv bd \ [m]$ et pour tout entier naturel n, $a^n \equiv b^n \ [m]$.

Démonstration. Il existe k et k' des entiers tels que $a = b + km$ et $c = d + k'm$. On a alors

- $a + c = b + d + (k + k')m$, ce qui prouve que $a + c \equiv b + d \ [m]$.
- $ac = (b + km)(d + k'm) = bd + (bk' + kd + kk')m$, ce qui prouve que $ac \equiv bd \ [m]$.

La seconde propriété se déduit immédiatement par récurrence. ■

Exemple

Soit $N = 2^{111} + 7$. Comme $2 \equiv -1 \ [3]$, on a $2^{111} \equiv (-1)^{111} \equiv -1 \ [3]$. Comme de plus $7 \equiv 1 \ [7]$, on déduit $N \equiv -1 + 1 \equiv 0 \ [3]$, ce qui montre que N est divisible par 3.

Exemple

Montrons que pour tout entier naturel n, $u_n = 3^n + 7^n - 2$ est divisible par 8. Vu que $7 \equiv -1 \ [8]$, on a $u_n \equiv 3^n + (-1)^n - 2 \ [8]$. Cela nous amène à envisager deux cas, selon la parité de n.

- Si n est pair, on peut l'écrire $n = 2k$, et on a alors $3^{2k} = 9^k \equiv 1^k \equiv 1 \ [8]$ ainsi que $(-1)^{2k} = 1$, donc $u_n \equiv 1 + 1 - 2 \equiv 0 \ [8]$.
- Si n est impair, on peut l'écrire $n = 2k + 1$. On a alors
$$3^{2k+1} = 9^k \times 3 \equiv 1^k \times 3 \equiv 3 \ [8]$$
et $(-1)^{2k+1} = -1$, donc $u_n \equiv 3 - 1 - 2 \equiv 0 \ [8]$.

Dans le deux cas, u_n est bien divisible par 8.

Exemple

Critère de divisibilité par 3, par 9.

Soit un entier N s'écrivant $\overline{a_n \ldots a_1 a_0}$ en base 10. Cela signifie que
$$N = a_n \times 10^n + \cdots + a_1 \times 10 + a_0$$
Comme $10 \equiv 1 \ [3]$, on en déduit que pour tout entier naturel p, on a $10^p \equiv 1^p \equiv 1 \ [3]$ et donc $N \equiv a_n + \cdots + a_1 + a_0 \ [3]$.

On retrouve la propriété bien connue qui affirme qu'un entier N est divisible par 3 si et seulement si la somme de ses chiffres $a_n + \cdots + a_1 + a_0$ l'est également.

Le critère est le même pour la division par 9.

Exemple

Montrons que l'équation $7x^2 - 3y^2 = 11$ n'a pas de solution en nombres entiers.

Réduisons modulo 3 pour faire disparaître l'une des lettres. On a
$$7x^2 - 3y^2 \equiv 7x^2 \equiv x^2 \ [3]$$
et $11 \equiv 2 \ [3]$, donc si $(x; y)$ est solution de cette équation, on a $x^2 \equiv 2 \ [3]$.

À l'aide d'un tableau, calculons toutes les valeurs possibles de x^2 modulo 3. Tout entier est congru soit à -1, soit à 0, soit à 1 modulo 3.

$x \equiv \ldots \ [3]$	-1	0	1
$x^2 \equiv \ldots \ [3]$	1	0	1

L'égalité $x^2 \equiv 2 \ [3]$ n'a donc jamais lieu, ce qui prouve que l'équation n'a pas de solution.

Exemple

Dans un triangle rectangle à côtés entiers, l'une des trois longueurs est divisible par 3.

En effet pour tout entier n, n^2 est congru à 0 ou à 1 modulo 3, selon que x est congru à 0 modulo 3 ou pas. Si aucun des côtés x, y, z n'est divisible par 3, l'égalité de Pythagore $x^2 = y^2 + z^2$ conduit à $1 \equiv 1 + 1 \ [3]$, ce qui est faux.