Divisibilité et congruences

1. Divisibilité dans $\mathbb{Z}$

a/ Quelques propriétés de $\mathbb{N}$

Théorème : tout sous-ensemble non vide de $\mathbb{N}$ possède un plus petit élément.
Démonstration : c'est très dur ! On l'admet
Corollaire[1] (principe de descente infinie) : il n'existe pas dans $\mathbb{N}$ de suite infinie strictement décroissante.
Démonstration à faire[2] :

b/ Notion de divisibilité

Définition : soient a et b deux entiers relatifs (c'est-à-dire dans $\mathbb{Z}$). S'il existe un entier relatif k tel que $a = k \cdot b$, on dit de manière équivalente que :

- a est un multiple de b ;
- b est un diviseur de a ;
- b divise a.

On note $b \mid a$.

Remarques et propriétés immédiates :

- 0 est un cas souvent problématique, ne pas oublier de le traiter, souvent à part.
- Pour tout entier relatif a de $\mathbb{Z}$, les entiers $0, a, -a, 2a, -2a, \ldots$ sont les multiples de a. L'ensemble de ces multiples est noté $a\mathbb{Z}$.
  Exemple à compléter : $3\mathbb{Z} =$
- Tout entier relatif a admet des diviseurs, au moins $1, -1, a, -a$ (si $a \neq 0$ pour les deux derniers).
- Un entier naturel (de $\mathbb{N}$) est un nombre premier si et seulement si il admet exactement deux diviseurs dans $\mathbb{N}$. Ceci exclut 0 et 1, qui ne sont pas premiers.
- Si $a \neq 0$, tout diviseur b de a vérifie $|b| \leq |a|$, car $a = k \cdot b$ avec $|k| \geq 1$.
- On en déduit immédiatement que tout entier non nul admet un nombre fini de diviseurs[3].

c/ Propriétés

Théorème : soient *a, b* et *c* trois entiers relatifs.

- Si $a \mid b$ alors $a \mid bc$;
- Si $a \mid b$ alors $ac \mid bc$;
- Si $a \mid b$ et $a \mid c$ alors :
  - $a \mid b + c$;
  - $a \mid b - c$;
  - et plus généralement a divise toute combinaison linéaire de b et c : $a \mid bu + cv$, où u et v sont deux entiers relatifs quelconques.
- Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

Démonstrations : faire en exercice la preuve de la combinaison linéaire

[1] Un corollaire est la conséquence « facile » d'un théorème principal. Un lemme est un petit théorème qui sert à démontrer un gros théorème.
[2] Preuve qui tient en une ligne…
[3] Constatez comme une propriété aussi évidente n'est pas si simple à démontrer.

Théorème : Si $a|b$ et $b|a$ alors $a = b$.

Démonstration 1 :

Remarquons que $a \neq 0$ (respectivement $b \neq 0$), sinon $a|b$ n'a pas de sens (respectivement $b|a$).

Puisque $a|b$ et $b|a$, il existe deux entiers relatifs k et k' tels que $a = kb$ et $b = k'a$.

Donc $ab = kk'ab$.

Comme $a \neq 0$ et $b \neq 0$, le produit ab est aussi différent de 0. On peut donc simplifier :

$$ab = kk'ab \Leftrightarrow kk' = 1 \Leftrightarrow \begin{cases} k = k' = 1 \text{ et } a = b \\ k = k' = -1 \text{ et } a = -b \end{cases}$$

CQFD

Démonstration 2 (plus élégante) :

Comme $a|b$ et , alors d'après une des propriétés du § 1b/, $|b| \leq |a|$ et $|a| \leq |b|$.

Donc $|a| = |b|$. ■

d/ Exemples et méthodes

Récurrence : Montrons que $\forall n \in \mathbb{N}, \quad 7|9^n - 2^n$

Initialisation : Pour $n = 0$, $9^0 - 2^0 = 0$ et $7|0$. La propriété est vraie au rang 0.

Hérédité : Supposons que pour un entier n fixé, $7|9^n - 2^n$ (hypothèse de récurrence)

Factorisons l'expression obtenue au rang $n + 1$, en faisant apparaître l'hypothèse de récurrence[4] :

$$9^{n+1} - 2^{n+1} = 2 \underbrace{\left(9^n - 2^n\right)}_{\text{divisible par 7 (HR)}} + \underbrace{7 \times 9^n}_{\text{divisible par 7}} \quad \text{(spoil 9 = 2 + 7)}$$

D'après les propriétés du § 1c/, une combinaison linéaire de deux nombres divisibles par 7 est divisible par 7. Donc la propriété est vraie au rang $n + 1$.

Conclusion : la propriété étant initialisée et héréditaire, on a montré par récurrence que $\forall n \in \mathbb{N}, \quad 7|9^n - 2^n$.

Raisonnement par disjonction des cas : montrons que $\forall n \in \mathbb{Z}, \quad 2|n(n+1)$

- Soit n est pair, et alors il existe $n' \in \mathbb{Z}$ tel que $n = 2n'$.
  Donc $n(n+1) = 2n'(n+1)$ est divisible par 2
- Soit n est impair, et alors il existe $n' \in \mathbb{Z}$ tel que $n = 2n' + 1$.
  Donc $n(n+1) = n(2n'+1+1) = 2n(n'+1)$ est divisible par 2 ■

Utilisation de connaissances/astuces de calcul : Montrons que $\forall n \in \mathbb{N}, \quad 4|5^n + 19$.

Le cas $n = 0$ est trivial, supposons pour la suite $n \neq 0$.

$$5^n + 19 = 5^n - 1 + 20$$

$$= (5-1)\left(5^{n-1} + 5^{n-2} + \ldots + 5 + 1\right) + 20 \quad \text{d'après } 1 + q + q^2 + \ldots + q^n = \frac{q^{n+1} - 1}{q - 1}$$

[4] L'idée est de forcer la factorisation sur un des deux termes du rang $n + 1$, et de voir ce qu'il reste ou ce qu'il faut enlever. Faites le calcul en factorisant par 9 et non par 2 : vous constaterez que la méthode fonctionne tout aussi bien.

$= 4\left(5^{n-1}+5^{n-2}+\ldots+5+1\right)+4\times 5$, qui est divisible par 4 par combinaison linéaire ■

Exercice : reprendre les exemples 1 et 3 ci-dessus en échangeant les méthodes.

Utilisation des propriétés du cours (divisibilité d'une combinaison linéaire ici, c'est très puissant)

- Trouvons les entiers naturels n tels que n divise $n + 8$.
  Comme $n \mid n$ et $n \mid n+8$, alors $n \mid n+8-n$. Donc $n \mid 8$, $n \in \{1,2,4,8\}$.
  Le raisonnement précédent est une implication $(\Rightarrow)$, il faut donc faire la réciproque.
  Réciproquement, si $n \in \{1,2,4,8\}$, alors $n+8$ est respectivement égal à 9, divisible par 1, puis 10, divisible par 2, puis 12 divisible par 8, et enfin 16, divisible par 8.
  Donc $S = \{1,2,4,8\}$
- Trouvons les entiers naturels n tels que $n - 4$ divise $3n + 24$. *A compléter !*
  Même principe que le précédent, en un peu plus compliqué. Les détails sont laissés au lecteur.
  $n-4 \mid n-4$ et $n-4 \mid 3n+24 \quad \Rightarrow \quad n-4 \mid 3n+24-3(n-4) \quad \Rightarrow n-4 \mid 36$
  Donc $n-4 \in \{-4,-3,-2,-1,1,2,3,4,6,9,12,18,36\}$. Pourquoi a-t-on des nombres négatifs dans cet ensemble ? On en déduit ensuite les valeurs de n : $n \in \{$
  Comme précédemment, on étudie la réciproque.
  On peut le faire par combinaison linéaire également :
  $n-4 \mid n-4$ et $n-4 \mid 36 \quad \Rightarrow \quad n-4 \mid 3(n-4)+36 \quad \Rightarrow$
- Trouvons les entiers a tels que $a \mid 42n+37$ et $a \mid 7n+4$.
  A faire en s'inspirant des exemples précédents. Pour un des cas de la réciproque, il est plus simple de trouver un exemple où « ça marche ».

e/ <u>La division euclidienne</u>

Théorème : soient a et b deux entiers naturels non nuls[5] (donc dans $\mathbb{N}^*$).

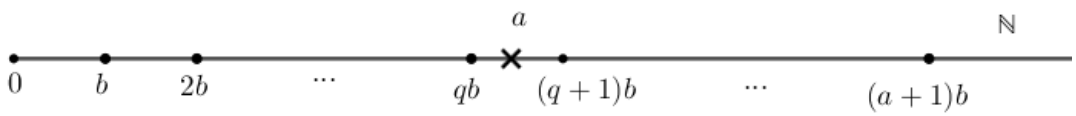
Alors il existe un unique couple $(q;r)$ d'entiers naturels tels que $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$.

Vocabulaire :

- Calculer q et r est effectuer la division euclidienne de a par b ;
- a est le dividende ;
- b est le diviseur ;
- q est le quotient ;
- r est le reste.

Démonstration (essayez de la comprendre mais ne passez pas trop de temps dessus) :

Existence : écrivons les multiples successifs de b sur un axe gradué :



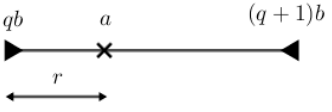
On considère l'ensemble des multiples de b strictement supérieurs à a.

Comme $(a+1)b > a$, cet ensemble est non vide. D'après le théorème du § 1a, il admet un plus petit élément.

Supposons que cet élément soit $(q+1)b$.

Alors on a $qb \le a < (q+1)b$ (pourquoi n'a-t-on pas $a < qb$?)

[5] La définition reste juste avec simplement $b \neq 0$, mais n'a que peu d'intérêt dans ce cas.



Si $a = qb$ alors $r = 0$.

Sinon $a \in]qb;(q+1)b[$. Posons dans ce cas $r = a - qb$.

D'une part, on a $r > 0$ car $a > qb$.

D'autre part $r = a - qb$ et $a < (q+1)b$ donne $r < (q+1)b - qb \Leftrightarrow r < b$.

L'existence du couple $(q;r)$ est prouvée.

Unicité : la preuve se fait par l'absurde, ce qui est souvent le cas pour l'unicité.

Supposons qu'il existe deux couples différents $(q_1;r_1)$ et $(q_2;r_2)$ tels que :

$a = bq_1 + r_1 \quad 0 \le r_1 < b$ et $a = bq_2 + r_2 \quad 0 \le r_2 < b$

On obtient alors avec les encadrements sur les restes[6] : $-b < r_2 - r_1 < b$;

Et avec en soustrayant les divisions euclidiennes $r_2 - r_1 = b(q_1 - q_2)$.

On en déduit que $r_2 - r_1$ est un multiple de b, qui est dans l'intervalle $]-b;b[$. le seul multiple de b dans cet intervalle est 0. Donc $r_1 = r_2$, que l'on notera r pour la suite.

On en déduit que $a - r = bq_1$ et $a - r = bq_2$.

Donc $bq_1 = bq_2$. Comme $b \neq 0$, on obtient en divisant par b : $q_1 = q_2$.

L'unicité est prouvée. ■

Théorème : soient a un entier relatif, et b un entier naturel non nul.

Alors il existe un unique couple $(q;r)$, avec q relatif et r naturel, tels que $\begin{cases} a = bq + r \\ 0 \le r < b \end{cases}$.

Le vocabulaire est le même que ci-dessus.

2. Les congruences

Les congruences ne sont qu'une notation pratique pour la division euclidienne, et sa généralisation.

a/ Définition

Définition : soit n un entier naturel supérieur ou égal à 2, soient deux entiers relatifs a et b. 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 en général $a \equiv b[n]$, parfois $a \equiv b(n)$, $a \equiv b(\text{mod } n)$ ou $a = b[n]$.

Exemple : l'heure de la sieste $14 \equiv 2[12]$.

Théorème : $\forall (a,b) \in \mathbb{Z}^2, \forall n \in \mathbb{N}, n \ge 2 : \quad a \equiv b[n] \Leftrightarrow n | a - b$

Démonstration : évidente, à faire quand même !

Remarque : on raisonne toujours avec des entiers lorsque l'on utilise des congruences.

b/ Compatibilité avec les opérations

Théorème : soient *a, b*, *c* et *d* des entiers relatifs, *n* un entier naturel supérieur ou égal à 2, *p* un entier naturel quelconque.

Si $a \equiv b[n]$ et $c \equiv d[n]$ alors :

- $a + c \equiv b + d[n]$

[6] Attention : on ne soustrait jamais deux encadrements. On passe à l'opposé sur le deuxième encadrement, et on ajoute les encadrements obtenus

- $a-c\equiv b-d\left[n\right]$
- $ac\equiv bd\left[n\right]$
- $a^p\equiv b^p\left[n\right]$

Remarque : et le quotient ?
Démonstrations :

- Pour $a+c\equiv b+d\left[n\right]$:

  Comme $a\equiv b\left[n\right]$ et $c\equiv d\left[n\right]$, d'après le théorème du § 2a, il existe k et k' tels que $a-b=kn$ et $c-d=k'n$.

  Donc $a+c-\left(b+d\right)=\left(k+k'\right)n$. Toujours d'après le théorème du § 2a, ceci équivaut à $a+c\equiv b+d\left[n\right]$.
- La preuve de $a-c\equiv b-d\left[n\right]$ est quasi identique.
- Pour $ac\equiv bd\left[n\right]$, il faut adapter un peu… je vous laisse réfléchir ☺

- la preuve de $a^p\equiv b^p\left[n\right]$ se fait par récurrence à partir du produit, faire au brouillon l'hérédité.

Exemple : il est 15 heures, quelle heure était-il il y a 173 heures ?
Remarque et contre-exemples : la propriété $a\equiv b\left[n\right]\Rightarrow a^p\equiv b^p\left[n\right]$ n'est pas une équivalence.

- $8^2\equiv 10^2\left[36\right]$ mais 8 n'est pas congru à 10 (ni à -10 si on pense à $-\sqrt{n}$) modulo 36.
- $7^2\equiv 11^2\left[36\right]$ mais 8 n'est pas congru à 11 (ni à -11 si on pense à $-\sqrt{n}$) modulo 36

c/ <u>Exemples et méthodes</u>
Bien sûr, la calculatrice est interdite…

- Quel est le reste de 50^{100} dans la division euclidienne par 7 ?
  On remarque que $50\equiv 1\left[7\right]\Rightarrow 50^{100}\equiv 1^{100}\left[7\right]\Rightarrow 50^{100}\equiv 1\left[7\right]$, le reste vaut 1.
- Quel est le reste de 23^{41} dans la division euclidienne par 7 ?
  On cherche une puissance de 23 congrue à 1 modulo 7.
  On part de $23\equiv 2\left[7\right]$.

  On en déduit que $23^2\equiv 2^2\left[7\right]\Leftrightarrow 23^2\equiv 4\left[7\right]$ puis $23^3\equiv 4\times 2\left[7\right]\Leftrightarrow 23^3\equiv 1\left[7\right]$.

  On effectue la division euclidienne de l'exposant 41 par la puissance trouvée 3 : $41=3\times 13+2$

  D'où $23^{41}\equiv 23^{3\times 13+2}\equiv\left(23^3\right)^{13}\cdot 23^2\equiv 1^{13}\cdot 2^2\equiv 4\left[7\right]$. Le reste est 4.
- Avec des entiers négatifs dans les congruences : montrer que $1^{2021}+2^{2021}+3^{2021}+4^{2021}$ est divisible par 5. Généraliser.

On a :

- $1^{2021} \equiv 1[5]$
- $2^{2021} \equiv 2^{2021}[5]$
- $3^{2021} \equiv (-2)^{2021}[5] \equiv -2^{2021}[5]$ → on a remarqué que $5 = 3+2$
- $4^{2021} \equiv (-1)^{2021}[5] \equiv -1^{2021}[5]$

D'où $1^{2021} + 2^{2021} + 3^{2021} + 4^{2021} \equiv 1^{2021} + 2^{2021} - 2^{2021} - 1^{2021} \equiv 0[7]$

- Généralisation ?

3. UNE APPLICATION : CRITÈRES DE DIVISIBILITÉ

On note les entiers avec une barre par dessus pour faire apparaître leur décomposition dans le système décimal (base 10) : $\overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots 10 \cdot a_1 + a_0$.

Pour trouver un critère de divisibilité, on simplifie l'écriture d'un nombre grâce aux congruences modulo le diviseur.

Exemples :

- Critère de divisibilité par 9

  Comme $10 \equiv 1[9]$, puis $10^n \equiv 1^n[9] \equiv 1[9]$ par puissance, on en déduit que

  $\overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots 10 \cdot a_1 + a_0 \equiv a_n + a_{n-1} + \ldots a_1 + a_0[9]$

  Donc un entier est divisible par 9 si la somme de ses chiffres est divisible par 9
- Critères de divisibilité par 3 et par 5 : *à faire sur le modèle du critère de divisibilité par 9*

- Critère de divisibilité par 4

  Comme $10^2 \equiv 0[4]$, puis $10^n \equiv 0[4]$ pour $n \geq 2$ par produit, on en déduit que

  $\overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots 10 \cdot a_1 + a_0 \equiv 10 \cdot a_1 + a_0[4]$

  Donc un entier est divisible par 4 si et seulement si le nombre composé de ses deux derniers chiffres est divisible par 4.

  raisonnement similaire pour la divisibilité par 8.
- Critère de divisibilité par 11

  Comme $10 \equiv -1[11]$ et $10^2 \equiv 1[11]$, on en déduit que $10^{2n} \equiv 1[11]$ et $10^{2n+1} \equiv -1[11]$ d'où

  $\overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \ldots 10 \cdot a_1 + a_0 \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \ldots - a_1 + a_0[11]$

  Donc un entier est divisible par 11 si la somme alternée de ses chiffres est divisible par -11
- Critère de divisibilité par 7, par 13, … : ça se complique ! mais on peut toujours raisonner comme ci-dessus.

  Une autre méthode pour un critère pour la divisibilité par 7 : montrer que si un entier n de la forme $n = 10a + b$ est divisible par 7, alors le nombre $a - 2b$ est divisible par 7 (*indice* : se fait en une seule congruence par produit)

Application : pour 25718, itérer le processus jusqu'à obtenir un nombre simple.