Arithmétique modulaire

Plan du chapitre

Introduction

Introduction...

Dans ce chapitre nous travaillerons exclusivement avec des nombres entiers. Voici une première propriété utile pour la suite :

Propriété 1 : Somme et produit d'entiers

La somme et le produit de deux nombres entiers est un nombre entier.
C'est-à-dire, pour tout $a, b \in \mathbb{Z}$ on a :

$$a+b \in \mathbb{Z} \quad \text{et} \quad ab \in \mathbb{Z}$$

Partie I Divisibilité dans $\mathbb{Z}$

A - Multiples et diviseurs d'un entier

Définition 1 : Multiple

Pour $a, b \in \mathbb{Z}$, on dit que a est un **multiple** de b s'il existe un entier k tel que :

$$a = bk$$

À retenir : Comme vous aimez bien le dire, « a est dans la table de multiplication de b ».
On notera l'ensemble des multiples de a : $a\mathbb{Z} = \{ak \ / \ k \in \mathbb{Z}\}$

Attention : On ne justifiera jamais qu'un nombre est multiple d'un autre à l'aide de la phrase précédente !

Exemple :

- 15 est un multiple de 5 car $15 = 5 \times 3$
- 15 est un multiple de 3 car $15 = 3 \times 5$
- -63 est un multiple de 7 car $-63 = 7 \times (-9)$

Propriété 2 : Somme de multiples

La somme de deux multiples, d'un entier a, est un multiple de a.

Exemple :

Considérons n et m, deux multiples de 3.
Ainsi $n = 3k_1$ où $k_1 \in \mathbb{Z}$ et $m = 3k_2$ où $k_2 \in \mathbb{Z}$.
On a alors :

$$\begin{aligned} n+m &= 3k_1 + 3k_2 \\ &= 3(k_1+k_2) \end{aligned}$$

Or on sait que $k_1 + k_2 \in \mathbb{Z}$ donc $n+m$ est bien un multiple de 3.

Démonstration :

La démonstration dans le cas général va suivre le même schéma.
Considérons n et m, deux multiples de a.
Ainsi $n = ak_1$ où $k_1 \in \mathbb{Z}$ et $m = ak_2$ où $k_2 \in \mathbb{Z}$.

On a alors :

$$\begin{aligned} n+m &= ak_1 + ak_2 \\ &= a(k_1+k_2) \end{aligned}$$

Or on sait que $k_1+k_2 \in \mathbb{Z}$ donc $n+m$ est bien un multiple de a. ■

Propriété 3 : Produit de multiples

Le produit de deux multiples, d'un entier a, est un multiple de a.

Démonstration :

Laisser en exercice.

.....

.....

.....

.....

.....

.....

.....

.....

■

Définition 2 : Diviseur

Pour $a, b \in \mathbb{Z}$, on dit que b est un **diviseur** de a s'il existe un entier k tel que :

$$a = bk$$

Information : On a la même définition que pour un **multiple** sauf qu'ici nous nous intéressons plus au même entier.

À retenir : On retiendra facilement l'entier jouant le rôle de diviseur, en effet dans le cas où $b \neq 0$ l'égalité :

$$a = bk \Leftrightarrow \frac{a}{b} = k$$

Exemple :

- -7 est un diviseur de 21 car $21 = (-7) \times (-3)$
- 11 est un diviseur de 275 car $275 = 11 \times 25$

Propriété 4 : Opposé

Pour $n \in \mathbb{Z}$ on a :

Si a est un diviseur de n alors $-a$ est aussi un diviseur de n.

Démonstration :

Soient $n \in \mathbb{Z}$ et $a \in \mathbb{Z}$ un diviseur de n.

Donc :

il existe $k \in \mathbb{Z}$, tel que : $n = ak$

On a alors :

$$n = (-a) \times (-k)$$

De plus, comme $k \in \mathbb{Z}$ on a aussi $-k \in \mathbb{Z}$, on a alors $-a$ est aussi un diviseur de n. ■

À savoir faire 1 : Diviseurs/ multiples

1. Répondez aux questions suivantes :
   (a) Quels sont les entiers tels que 0 soit un de leurs multiples ?
   Tous les entiers, en effet pour tout $n \in \mathbb{Z}$ on a :
   $$0 = n \times 0 \quad \text{où } 0 \text{ est bien un entier}$$
   (b) Quels sont les multiples de 0 ?
   0 possède un unique multiple qui est 0 lui même, car :
   $$0 = 0 \times k \quad \text{pour tout } k \in \mathbb{Z}$$
   (c) Quels sont les diviseurs de 0 ?
   Tous les entiers, par la question 1) car :
   $$n \text{ est un multiple de 0 si, et seulement si, 0 est un diviseur de } n.$$
2. Montrer que pour tout $n \in \mathbb{Z}$ on a que $n-1$ est un diviseur de $2n^2+4n-6$.
   Concrètement on cherche à montrer que $2n^2+4n-6 = (n-1)k$ où $k \in \mathbb{Z}$.
   Factoriser $2n^2+4n-6$ pourrait être une bonne idée.
   On a :
   $$2n^2+4n-6 = 2\left(n^2+2n-3\right)$$
   De plus on remarque que 1 est racine évidente du polynôme X^2+2X-3 donc d'après le lien coefficients-racines, étant un polynôme unitaire, en notant r_2 la seconde racine de notre polynôme on a :
   $$-3 = 1 \times r_2$$
   $$r_2 = -3$$
   D'où $n^2+2n-3 = (n-1)(n+3)$.
   Ainsi on a :
   $$2n^2+4n-6 = 2(n-1)(n+3) = (n-1) \times 2(n+3) = (n-1)K$$
   où $K = 2(n+3) \in \mathbb{Z}$ car $n \in \mathbb{Z}$.
   D'où $n-1$ est bien un diviseur de $2n^2+4n-6$ pour tout $n \in \mathbb{Z}$.

Propriété 5 : Ensemble des diviseurs

Donnons deux propriétés utile pour déterminer l'ensemble des diviseurs d'un nombre entier donné.

1. Tout entier non nul n admet un nombre fini de diviseurs compris entre $-n$ et n.
   Pour tout diviseur d de $n \neq 0$ on a $|d| \leq |n|$.
2. Pour n, p et q des entiers naturels tels que $n = pq$, on a :
   $$p \leq \sqrt{n} \quad \text{ou} \quad q \leq \sqrt{n}$$

Démonstration :

1. Soit $n \in \mathbb{Z}^*$, considérons $d \in \mathbb{Z}$ un diviseur de n. On a alors :

$$n = dk \quad \text{où } k \in \mathbb{Z}$$

Comme $n \neq 0$ on a alors $k \neq 0$. Ainsi $|k| \geq 1$, car k est un entier.
D'où :

$$|d| = \left|\frac{n}{k}\right| = \frac{|n|}{|k|} \leq |n|$$

Ainsi :

$$-|n| \leq d \leq |n|$$

■

2. Considérons n, p et q trois entiers naturels tels que :

$$n = pq$$

Deux cas s'offrent à nous :

- **ou bien $p \leq q$**
  On a alors :
  $$p \leq q \Rightarrow p^2 \leq pq = n \Rightarrow p \leq \sqrt{n}$$
  Attention ici on utilise grandement le fait que p et n soient positifs.
- **ou bien $q \leq p$**
  Ce cas est complétement symétrique et nous permet de démontrer que $q \leq \sqrt{n}$.

■

À savoir faire 2 : Ensemble des diviseurs

1. Quels sont les diviseurs de 1 ? 1 et -1 grâce à la première partie de la propriété précédente.
2. Déterminer la liste des diviseurs positifs de 84.
   Déterminer la liste des diviseurs positifs de 84 c'est déterminer l'ensemble des entiers positifs p tels que :

$$84 = pq \quad \text{où } q \in \mathbb{N}$$

Or on sait d'après la propriété précédente que si l'on arrive à décomposer 84 de la sorte au moins l'un des deux facteurs est $\leq \sqrt{84}$.
Donc il nous suffit de déterminer toutes les décompositions de 84 avec l'un des facteurs étant ≤ 84, pour obtenir toutes les décompositions de 84 sous la forme de produit de deux entiers.

- **Étape 1 :** Déterminer une valeur approché de : $\sqrt{84}$.
  $\sqrt{84} \simeq 9$ car $81 \leq 84 \leq 100$.
- **Étape 2 :** Décomposer 84 à l'aide des entiers ≤ 9.
  - $84 = 1 \times 84$
  - $84 = 2 \times 42$
  - $84 = 3 \times 28$
  - $84 = 4 \times 21$
  - $84 = 6 \times 14$
  - $84 = 7 \times 12$
- **Étape 3 :** On lit alors la liste des diviseurs de 84.

$$\mathscr{D}_{84}^{+} = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

3. Et la liste de tous les diviseurs de 84 ?
   En combinant le résultat précédent et la première partie de la propriété précédente on a que tous les diviseurs de 84 sont comprit entre -84 et 84 de plus si d est un diviseur de 84 on a aussi $-d$ un diviseur de 84. Ainsi l'ensemble des diviseurs de 84 est :

$$\mathscr{D}_{84} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 7, \pm 12, \pm 14, \pm 21, \pm 28, \pm 42, \pm 84\}$$

B - Relation de divisibilité

Définition 3 : Divise

Pour $a, b \in \mathbb{Z}$, on dit que b **divise** a s'il existe un entier k tel que :

$$a = bk$$

On notera cela $b \mid a$ (se lit « b divise a ») .

À retenir : Encore la même définition.
On récapitule on a alors :

a est un multiple de b **si, et seulement si,** b est un diviseur de a **si, et seulement si,** b divise a.

Information : On dit également que ***a* est divisible par *b***.

Point chaud : 0 divise 0 ?
D'après la définition précédente, 0 divise 0.
En effet, il existe bien $k \in \mathbb{Z}$ tel que $0 = k \times 0$ (prendre n'importe quel entier k fonctionne). Ainsi, il n'y a aucun problème à dire que 0 divise 0.
Cependant, il faut distinguer les expressions « 0 divise 0 » et « 0 divisé par 0 ».
Même si les deux phrases emploient les mêmes mots, elles ne signifient pas la même chose :

- « 0 divise 0 » a un sens bien défini en arithmétique (car la condition est vérifiée pour tout k),
- tandis que « 0 divisé par 0 » n'a pas de sens (l'opération de division par 0 est indéfinie).

Cela peut sembler abstrait, car elles paraissent proches dans le langage courant, mais la différence est importante : l'une a un sens logique, l'autre non.
On peut tout de même donner une propriété pour unifier ces deux notions (dans un cas particulier).

Propriété 6 : Unification des notions

Pour $a, b \in \mathbb{Z}$,
On dit que b divise a s'il existe $k \in \mathbb{Z}$ tel que :

$$a = bk$$

Si, de plus, l'égalité précédente n'est vérifiée que par un **unique** entier k, on peut alors définir la division de a par b :

$$\frac{a}{b} \text{ (notre fameux } a \text{ divisé par } b)$$

et ce quotient est égal à notre unique k.

Propriété 7 : Réflexivité - Transitivité

- **Réflexivité :** Pour tout $a \in \mathbb{Z}$, on a $a \mid a$;
- **Transitivité :** Pour tout $a, b, c \in \mathbb{Z}$

$$\textbf{Si} \quad a \mid b \text{ et } b \mid c \quad \textbf{alors} \quad a \mid c$$

À retenir :

- La réflexivité peut paraître évidente et inutile mais elle sera d'une grande aide dans certaines démonstration lorsque l'on va chercher à démontrer à l'aide de la relation divise.
- La transitivité nous assure que la relation divise ne se brise pas en chaîne.

À savoir faire 3 : Utiliser la transitivité

Démontrer que 11 divise 1760.
Comme $176 \mid 1760$ en effet : $1760 = 176 \times 10$ et que $11 \mid 176$ en effet : $176 = 11 \times 16$.
On a alors d'après la transitivité de la relation divise : $11 \mid 1760$.

Démonstration :

- **Réflexivité :** Soit $a \in \mathbb{Z}$, il est clair que $a = a \times 1$ où $1 \in \mathbb{Z}$ donc $a \mid a$. ■
- **Transitivité :** Soit $a, b, c \in \mathbb{Z}$, tels que :

$$a \mid b \quad \text{et} \quad b \mid c$$

C'est-à-dire il existe $k_1, k_2 \in \mathbb{Z}$ tels que :

$$b = ak_1 \quad \text{et} \quad c = bk_2$$

On a alors :

$$c = bk_2 = ak_1k_2 = aK \quad \text{où } K = k_1k_2 \in \mathbb{Z}$$

D'où $a \mid c$ ■

Propriété 8 :

Pour tout $a, b \in \mathbb{Z}$, on a :

$$a \mid b \text{ et } b \mid a \quad \Leftrightarrow \quad a = \pm b$$

Démonstration :

Soit $a, b \in \mathbb{Z}$,

$\Leftarrow$ Ce sens est évident, supposons que $a = \pm b$ on a bien :

- $a \mid \pm a$ car $\pm a = a \times (\pm 1)$
- $\pm a \mid a$ car $a = \pm a \times (\mp 1)$

$\Rightarrow$ Supposons maintenant que $a \mid b$ et $b \mid a$ et $a, b \neq 0$, on a alors que :

- a est un diviseur de b donc par la propriété 5 on a : $|a| \leq |b|$;
- b est un diviseur de a donc par la propriété 5 on a : $|b| \leq |a|$;

On conclut de ces deux points que : $|a| = |b| \Rightarrow a = \pm b$
Dans le cas où $a = 0$ ou $b = 0$, comme ces deux cas sont symétriques traitons un seul des deux cas : $a = 0$.
On a alors $0 \mid b$, c'est-à-dire il existe $k \in \mathbb{Z}$ tel que :

$$b = 0 \times k = 0$$

D'où $a = \pm b$. ■

Théorème 1 : Combinaison linéaire

Soit $a, b, c \in \mathbb{Z}$,

Si $a \mid b$ et $a \mid c$ **alors** pour tout $u, v \in \mathbb{Z}$, $a \mid ub + vc$

Information : Le dernier théorème est même une équivalence.
En effet on démontre la réciproque en considérant le cas $u = 1$ et $v = 0$ pour démontrer que $a \mid b$ et le cas $u = 0$ et $v = 1$ pour démontrer que $a \mid c$.

À retenir : Combinaison linéaire
Pour $x, y \in \mathbb{R}$, on appelle combinaison linéaire de x et y tout expression de la forme :

$$ax + by \quad \text{où } a, b \in \mathbb{Z}$$

C'est une expression construite à partir d'un ensemble de termes en multipliant chacun de ces termes par une constante et les ajoutant entre eux.

Démonstration :

Soit $a, b, c \in \mathbb{Z}$,
Supposons que $a \mid b$ et que $a \mid c$ on a alors :

$$\begin{cases} b = ak_1 \\ c = ak_2 \end{cases} \quad \text{où } k_1, k_2 \in \mathbb{Z}$$

Soit $u, v \in \mathbb{Z}$, on a alors :

$$\begin{aligned} ub + vc &= uak_1 + vak_2 \\ &= a(uk_1 + vk_2) \\ &= aK \quad \text{où } K = uk_1 + vk_2 \end{aligned}$$

Comme $K = uk_1 + vk_2 \in \mathbb{Z}$, on vient alors de montrer que $a \mid ub + vc$ ■

À retenir : En particulier : si $a \mid b$ et $a \mid c$ alors $a \mid b + c$ et $a \mid b - c$.

Exemple :

Soit $n \in \mathbb{Z}$, démontrer que :

$$\text{si } a \mid n-4 \text{ et } a \mid n-7 \text{ alors } a \mid 3$$

En appliquant le théorème précédent avec $u = 1$ et $v = -1$ alors on a :

$$\begin{cases} a \mid n-4 \\ a \mid n-7 \end{cases} \Rightarrow a \mid n-4-(n-7) \Leftrightarrow a \mid 3$$

À savoir faire 4 : Résolution dans $\mathbb{Z}$ ou $\mathbb{N}$

1. Déterminer l'ensemble des entiers x tels que :

$$x - 1 \mid x + 3$$

Nous allons raisonner par analyse-synthèse :
Analyse : Considérons $x \in \mathbb{Z}$ tel que :

$$x - 1 \mid x + 3$$

Déterminer l'ensemble des diviseurs entiers de $x - 3$ n'est pas chose aisée... On préférerait plutôt avoir à déterminer la liste des diviseurs d'un nombre entier. Cherchons alors à transfomer $x - 1 \mid x + 3$ en $x - 1$

divisant un entier.
Grâce à la fameuse réflexivité on va créer une deuxième relation de divisibilité :

$$\begin{cases} x-1 \mid x+3 \\ x-1 \mid x-1 \end{cases}$$

En appliquant le théorème précédent avec $u=1$ et $v=-1$ on a :

$$\begin{cases} x-1 \mid x+3 \\ x-1 \mid x-1 \end{cases} \Rightarrow x-1 \mid x+3-x+1 \Leftrightarrow x-1 \mid 4$$

On vient alors de montrer que si x est solution de problème alors $x-1$ est un diviseur de 4.
C'est-à-dire $x-1 \in \mathscr{D}_4 = \{\pm 1, \pm 2, \pm 4\}$, donc $x \in \{-3,-1,0,2,3,5\}$. Grâce à cette phase d'analyse on vient de montrer que les seules solutions possibles à notre problème sont $-3,-1,0,2,3$ ou 5.
C'est-dire $\mathscr{S} \subset \{-3,-1,0,2,3,5\}$.
Synthèse : Vérifions si $-3,-1,0,2,3$ ou 5 sont solutions de notre problème.

- Pour $x=-3$ on a $x-1=-4$ et $x+3=0$ ainsi on a bien $x-1 \mid x+3$ d'où $-3 \in \mathscr{S}$;
- Pour $x=-1$ on a $x-1=-2$ et $x+3=2$ ainsi on a bien $x-1 \mid x+3$ d'où $-1 \in \mathscr{S}$;
- Pour $x=0$ on a $x-1=-1$ et $x+3=3$ ainsi on a bien $x-1 \mid x+3$ d'où $0 \in \mathscr{S}$;
- Pour $x=2$ on a $x-1=1$ et $x+3=5$ ainsi on a bien $x-1 \mid x+3$ d'où $2 \in \mathscr{S}$;
- Pour $x=3$ on a $x-1=2$ et $x+3=6$ ainsi on a bien $x-1 \mid x+3$ d'où $3 \in \mathscr{S}$;
- Pour $x=5$ on a $x-1=4$ et $x+3=8$ ainsi on a bien $x-1 \mid x+3$ d'où $5 \in \mathscr{S}$;

D'où $\mathscr{S} = \{-3,-1,0,2,3,5\}$.

2. Résoudre l'équation $x^2-4y^2=20$ d'inconnues $x, y \in \mathbb{N}$.
Soit $x, y \in \mathbb{N}$, on a :

$$x^2-4y^2=20 \Leftrightarrow (x-2y)(x+2y)=20$$

Ainsi $x-2y$ et $x+2y$ comme étant deux entiers sont deux diviseurs de 20.
De plus comme $x+2y \geq 0$ on a alors que $x+2y$ est un diviseur positif de 20 lui même positif donc $x-2y$ est également un diviseur positif de 20.
On peut alors affirmer que $x-2y, x+2y \in \mathscr{D}_{20}^{+} = \{1,2,4,5,10,20\}$ tels que leur produit donne 20.
De plus comme, $x, y \in \mathbb{N}$ on a $x-2y \leq x+2y$.
Donc trois possibilités s'offrent à nous :

$$\begin{cases} x-2y=1 \\ x+2y=20 \end{cases} \text{ ou } \begin{cases} x-2y=2 \\ x+2y=10 \end{cases} \text{ ou } \begin{cases} x-2y=4 \\ x+2y=5 \end{cases}$$

$$\Leftrightarrow \begin{cases} x=10,5 \\ y=\ldots \end{cases} \text{ ou } \begin{cases} x=6 \\ y=2 \end{cases} \text{ ou } \begin{cases} x=4,5 \\ y=\ldots \end{cases}$$

$$\Leftrightarrow \emptyset \text{ ou } \begin{cases} x=6 \\ y=2 \end{cases} \text{ ou } \emptyset$$

D'où $\mathscr{S} = \{(6,2)\}$.

Propriété 9 : Produit entre relation divise

Soient a, b, c et d des entiers, on a :

Si $a \mid b$ et $c \mid d$ **alors** $ac \mid bd$

Démonstration :

Soient a, b, c et $d \in \mathbb{Z}$,

Supposons que $a \mid b$ et $c \mid d$ on a alors qu'il existe $k_1, k_2 \in \mathbb{Z}$ tels que : $\begin{cases} b = ak_1 \\ d = ck_2 \end{cases}$.

Donc :

$$bd = ak_1ck_2 = ack_1k_2 = acK \quad \text{où } K = k_1k_2 \in \mathbb{Z}$$

D'où $ac \mid bd$. ■

Partie II Division euclidienne

Cette partie trouve sa genèse dans le fait que la partie précédente nous a permis de définir la divisibilité mais ne nous a pas fourni un procédé efficace pour vérifier, étant donné deux entiers a et b, si b divse a ou non...
La réponse à ce problème est (vous l'aurez sûrement deviné) d'effectuer la division de a par b, mais pas au sens de calculer $\frac{a}{b}$ en tant que nombre rationnel, mais au sens de la division « avec reste » que vous avez appris à l'école primaire.

A - Les différents cas

A.1 - Division euclidienne dans $\mathbb{N}$

Axiome 1 : Plus petit élément

Toute partie non vide de $\mathbb{N}$, admet un plus petit élément.

Théorème 2 : Lemme d'Archimède

Pour tout entiers naturels x et y, tel que $x \neq 0$, il existe un entier naturel n tel que :

$$nx > y$$

Démonstration :

Soit $x, y \in \mathbb{N}$, tel que $x \neq 0$.
Comme $x \in \mathbb{N}^*$, on a alors $x \geq 1$ d'où :

$$xy \geq y \quad \text{car } y \geq 0$$

D'autre part on a :

$$\begin{aligned} & y + 1 > y \\ \Leftrightarrow\ & x(y+1) > xy \leq y \\ \Leftrightarrow\ & x(y+1) > y \end{aligned}$$

Or $y + 1 \in \mathbb{N}$, ainsi nous avons bien trouvé un entier naturel $n = y + 1$ tel que :

$$nx > y$$

■

Théorème 3 : Division euclidienne dans $\mathbb{N}$

Pour tous $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, il existe un unique couple d'entiers naturels (q, r) satisfaisant :

$$a = bq + r\,, \quad \text{avec } 0 \leq r < b$$

Démonstration :

► **Existence du couple (q,r) :**

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, la question première à se poser dans une division euclidienne est combien de fois b dans a?

Ainsi considérons l'ensemble :

$$E = \{n \in \mathbb{N} \,/\, bn > a\}$$

Pour obtenir ce fameux combien de fois b dans a, ce que l'on a appelé le quotient en primaire, il faut déterminer le plus petit élément de E (en espérant déjà qu'il existe) et lui soustraire 1.

Comme $b \in \mathbb{N}^*$ et $a \in \mathbb{N}$, d'après le **lemme d'Archimède** , il existe $n \in \mathbb{N}$ tel que :

$$bn > a$$

D'où $E \neq \emptyset$, comme partie de $\mathbb{N}$ on a alors d'après l'axiome du plus petit élément que E possède un plus petit élément. Notons le q'.

On peut assurer que $q' \leq 1$ car sinon $q' = 0$ et on aurait :

$$a < b \times 0 = 0$$

Ce qui contredit le fait que $a \in \mathbb{N}$.

En considérant alors $q = q' - 1$ on a alors :

$$q \notin E \text{ car } q < q' \text{ et cela contredirait la propriété de plus petit élément de } E \text{ de } q'.$$

Donc $bq \leq a < b(q+1)$. Ainsi en posant $r = a - bq$ on a :

$$\begin{cases} a = bq + r \\ 0 \leq a - bq < b \end{cases} \Leftrightarrow \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

On vient alors de construire un couple d'entiers naturels (q,r) vérifiant les conditions souhaitées.

► **Unicité du couple (q,r) :**

Pour démontrer l'unicité du couple (q,r) vérifiant les conditions souhaitées, supposons par l'absurde que le couple n'est pas unique et donc nous pouvons considérer deux couples d'entiers (q,r) et (q',r') tels que :

$$\begin{cases} a = bq + r, & \text{avec } 0 \leq r < b \\ a = bq' + r', & \text{avec } 0 \leq r' < b \end{cases}$$

On a alors :

$$(L_1) - (L_2) \Leftrightarrow b(q - q') + r - r' = 0 \Leftrightarrow b(q - q') = r' - r$$

Or, on sait que :

$$\begin{cases} -b < -r \leq 0 \\ 0 \leq r' < b \end{cases} \Rightarrow -b < r' - r < b$$

On a alors :

$$-b < b(q - q') < b \Leftrightarrow -1 < q - q' < 1 \quad \text{car } b > 0$$

Comme $q - q' \in \mathbb{Z}$, on a alors :

$$q - q' \in \mathbb{Z} \cap]-1, 1[\Leftrightarrow q - q' = 0 \Leftrightarrow q = q'$$

D'où :

$$r' - r = b(q - q') = 0 \Leftrightarrow r' = r$$

On vient alors de montrer que $q = q'$ et $r = r'$ ce qui contredit l'hypothèse de l'existence d'au moins deux couples distincts.

D'où le couple d'entiers naturels (q,r) vérifiant les conditions souhaitées est unique. ■

Définition 4 : Division euclidienne

Pour $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, effectuer la **division euclidienne** de a par b c'est déterminer le couple (q, r) tel que :

$$a = bq + r, \quad \text{avec } 0 \leq r < b$$

On appelle alors a le dividende, b le diviseur, q le quotient et r le reste.

Exemple :

Effectuer la division euclidiennne de :

- 58 par 17
  $58 = 17 \times 3 + 7$ de plus on a bien : $0 \leq 7 < 17$
- 10 par 4
  $10 = 4 \times 2 + 2$ de plus on a bien : $0 \leq 2 < 4$

À savoir faire 5 : Utiliser la division euclidienne pour faire une disjonction de cas

Soit $n \in \mathbb{N}$, montrer que $n^2 + n$ est pair.
Indice 1 : Considérer la division euclidienne de n par 2.
Indice 2 : On rappelle qu'un nombre pair est un multiple de 2.
D'après le théorème de la division euclidienne on sait qu'il existe $q \in \mathbb{N}$ tel que :

$$n = 2q \quad \text{ou} \quad n = 2q + 1$$

Considérons ces deux cas :

- ou bien : $n = 2q$
  On a alors : $n^2 + n = n(n+1) = 2q(2q+1) = 2 \times q(2q+1)$ d'où $n^2 + n$ est bien un multiple de 2 car $q(2q+1) \in \mathbb{Z}$.
- ou bien : $n = 2q + 1$
  On a alors : $n^2 + n = n(n+1) = (2q+1)(2q+2) = 2(q+1)(2q+1)$ d'où $n^2 + n$ est bien un multiple de 2 car $(q+1)(2q+1) \in \mathbb{Z}$.

On vient alors de montrer que pour tout $n \in \mathbb{N}$, $n^2 + n$ est pair.

A.2 - Division euclidienne d'un entier relatif par un entier naturel non nul

La division euclidienne de 37 par 11 nous donne :

$$37 = 11 \times 3 + 4, \quad \text{où } 0 \leq 4 < 11$$

Si on souhaite maintenant réaliser la division euclidienne de -37 par 11, on peut écrire :

$$-37 = 11 \times (-3) - 4$$

Malheureusement cette fois-ci nous avons $-4 < 0$ donc nous n'avons pas réalisé la division euclidienne de -37 par 11.
En pratique on retire 1 (ça veut dire ajouter -1) au quotient pour le donner (l'ajouter) au reste :

$$-37 = 11 \times (-3) - 1 \times 11 + 1 \times 11 - 4 = 11 \times (-4) + 11 - 4 = 11 \times (-4) + 7, \quad \text{où } 0 \leq 7 < 11$$

Erreur fréquente : Si r est le reste dans la division euclidienne de a par b il n'est surtout pas vrai de dire $-r$ est le reste dans la division euclidienne de $-a$ par b, en fait on a plutôt comme reste $b - r$

Théorème 4 : Division euclidienne de "$\mathbb{Z}$ par $\mathbb{N}^*$"

Pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple d'entiers (q,r) satisfaisant :

$$a = bq + r\,, \quad \text{avec } 0 \leq r < b$$

Démonstration :

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Deux possibles :

- **Cas 1 :** $a \geq 0$, ce cas est la division euclidienne sur $\mathbb{N}$ démontré dans le théorème précédent.
- **Cas 2 :** $a < 0$, de la même manière que pour la division euclidienne dans $\mathbb{N}$, découpons la preuve en deux parties. Une première partie d'existence du couple puis une partie d'unicité du couple.
  ▶ **Existence du couple (q,r) :** Si $a < 0$ on a alors $-a \in \mathbb{N}$ et on peut alors effectuer la division euclidienne de $-a$ par b, on a alors :
  $$-a = bq' + r', \quad \text{où } 0 \leq r' < b$$
  Deux cas s'offrent alors à nous :
  - Si $r' = 0$ on a alors :
    $$a = b(-q')$$
    En posant $q = -q'$, on a effectué la division euclidienne de a par b et on a démontré l'existence du couple $(q,r) = (-q', 0)$ vérifiant les conditions souhaitées.
  - Si $r' \neq 0$ on a alors :
    $$a = b(-q') - r'$$
    Comme $-b < -r' < 0$ nous n'avons pas notre division euclidienne.
    Pour cela on va utiliser un ajouter - compenser au niveau du "quotient" :
    $$a = b(-q' - 1 + 1) - r' = b(-q' - 1) + b - r' = bq + r, \quad \text{où } q = -q' - 1 \in \mathbb{Z} \text{ et } r = b - r'$$
    De plus $0 < b - r' < b$, d'où venons de réaliser la division euclidienne de a par b et on a démontré l'existence du couple $(q,r) = (-q' - 1, b - r')$ vérifiant les conditions souhaitées.

  D'où, même pour $a < 0$, il existe toujours un couple d'entiers (q,r) tel que :
  $$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$
  ▶ **Unicité du couple (q,r) :** Ce prouve exactement de la même manière que pour la division euclidienne dans $\mathbb{N}$.

■

À savoir faire 6 : Division euclidienne de "$\mathbb{Z}$ par $\mathbb{N}^*$"

Réaliser les divisions euclidienne de :

1. -54 par 7
   On a $54 = 7 \times 7 + 5$ donc $-54 = 7 \times (-7) - 5 = 7 \times (-8) + 2$. On a alors :
   $$\boxed{-54 = 7 \times (-8) + 2}$$
2. -48 par 5
   On a $48 = 5 \times 9 + 3$ donc $-48 = 5 \times (-9) - 3 = 5 \times (-10) + 2$. On a alors :
   $$\boxed{-48 = 5 \times (-10) + 2}$$

A.3 - Division euclidienne dans $\mathbb{Z}$

Pour effectuer la division euclidienne de -37 par -11, aucune difficulté!
On sait que :

$$-37 = 11 \times (-4) + 7$$

Donc on a :

$$-37 = -11 \times 4 + 7$$

Mais dans ce cas là on a : $0 \leq 7 < |-11|$.

Théorème 5 : Division euclidienne dans $\mathbb{Z}$

Pour tous $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un unique couple d'entiers (q, r) satisfaisant :

$$a = bq + r\,, \quad \text{avec } 0 \leq r < |b|$$

Démonstration :

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$
Deux cas possibles :

- **Cas 1 :** $b > 0$, ce cas est la division euclidienne de "$\mathbb{Z}$ par $\mathbb{N}^*$" déjà démontré dans le théorème précédent, donc on sait qu'il existe un couple d'entiers (q, r) tel que :

  $$a = bq + r, \quad \text{où } 0 \leq r' < b = |b|$$

  On a même l'unicité de ce couple.

- **Cas 2 :** $b < 0$
  ▶ **Existence du couple (q, r) :** dans ce cas on considère $-b \in \mathbb{N}^*$ et on réalise la division euclidienne de a par $-b$:

  $$a = -bq' + r', \quad \text{où } 0 \leq r' < -b$$

  On a alors :

  $$a = b(-q') + r', \quad \text{où } 0 \leq r' < -b = |b|$$

  On vient alors de démontrer que, même pour $b < 0$, il existe un couple d'entiers $(q, r) = (-q', r')$ tel que :

  $$a = bq + r, \quad \text{où } 0 \leq r < |b|$$

  ▶ **Unicité du couple (q, r) :** Ce prouve exactement de la même manière que pour la division euclidienne dans $\mathbb{N}$.

■

On peut alors commencer à traduire les définitions de divisibilité à l'aide de notre nouvel outil.

Propriété 10 : Reste

b divise a si, et seulement si, le reste dans la division euclidienne de a par b est égal à 0.

Démonstration :

$\boxed{\Rightarrow}$ Supposons que b divise a alors il existe $k \in \mathbb{Z}$ tel que :

$$a = bk$$

D'où le reste dans la division euclidienne de a par b vaut 0.
$\boxed{\Leftarrow}$ Réciproquement supposons que le reste dans la division euclidienne de a par b vaut 0. Ainsi il existe $q \in \mathbb{Z}$ tel que :

$$a = bq$$

D'où par définition b divise a. ■

Exemple :

On a $6 \nmid 14$ car la division euclidienne de 14 par 6 nous assure :

$$14 = 6 \times 2 + 2$$

D'où le reste n'est pas égal à 0, donc 6 ne divise pas 14

À savoir faire 7 : Utiliser la division euclidienne pour justifier de la divisibilité d'un nombre par un autre

Montrer, de deux façons différentes, que pour tout $n \in \mathbb{N}$, l'entier $n^2 + n - 1$ n'est pas divisible par $n+2$.
Première méthode *(rapide)* : -2 n'est pas racine de $X^2 + X - 1$ donc ce polynôme n'est pas factorisable par $X+2$ d'où $n^2 + n - 1$ n'est pas divisible par $n+2$.
Deuxième méthode *(adapté à l'exercice)* : Fixons $n \in \mathbb{N}$,
En effectuant la division euclidienne de polynômes entre $X^2 + X - 1$ et $X + 2$ on obtient :

$$X^2 + X - 1 = (X+2)(X-1) + 1$$

D'où on a : $n^2+n-1 = (n+2)(n-1)+1$ ce qui est bien la division euclidienne de n^2+n-1 par $n+2$ car $0 \leq 1 < n+2$ car $n \in \mathbb{N}$.
Comme le reste est non nul, on peut affirmer que $n^2 + n - 1$ n'est pas divisible par $n+2$.

B - Nombres pairs, nombres impairs

Définition 5 : Nombre pair - impair

- Un nombre **pair** est un multiple de 2 ;
- Un nombre **impair** n'est pas pair.

Propriété 11 : Écriture

- Un nombre pair s'écrit sous la forme $2k$, avec $k \in \mathbb{Z}$;
- Un nombre impair s'écrit sous la forme $2k+1$, avec $k \in \mathbb{Z}$;

***Démonstration* :**

- Soit n un nombre pair, donc par définition n est un multiple de 2, donc il existe $k \in \mathbb{Z}$ tel que :

$$n = 2k$$

- Soit n un nombre impair, donc par définition n n'est pas pair, donc n n'est pas divisible par 2.
  Donc n ne possède pas 0 comme reste dans sa division euclidienne par 2, étant donné que les restes possible dans la division euclidienne par 2 sont : 0 ou 1.
  On peut alors affirmer que n possède 1 comme reste dans la division euclidienne par 2, d'où il existe $k \in \mathbb{Z}$ tel que :

$$n = 2k + 1$$

■

Propriété 12 : Carré

- Le carré d'un nombre pair est pair.
- Le carré d'un nombre impair est impair.

Démonstration :

- Soit n un entier pair, il existe alors $k \in \mathbb{Z}$ tel que :

$$n = 2k$$

Ainsi,

$$n^2 = (2k)^2 = 4k^2 = 2 \times 2k^2 \quad \text{où } 2k^2 \in \mathbb{Z}$$

D'où n^2 est pair.

- Soit n un entier impair, il existe alors $k \in \mathbb{Z}$ tel que :

$$n = 2k + 1$$

Ainsi,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \times \left(2k^2 + 2k\right) + 1 \quad \text{où } 2k^2 + 2k \in \mathbb{Z}$$

D'où n^2 est impair.

■

Propriété 13 : Somme/produit

- La somme de deux nombres pairs est un nombre pair. **PAIR + PAIR =PAIR**
- La somme de deux nombres impairs est un nombre pair. **IMPAIR + IMPAIR =PAIR**
- La somme d'un nombre pair et d'un nombre impair est un nombre impair. **PAIR + IMPAIR =IMPAIR**
- Le produit de deux nombres impairs est un nombre impair. **IMPAIR × IMPAIR =IMPAIR**
- Le produit d'un nombres pair et d'un nombre est un nombre pair. **PAIR × NOMBRE =PAIR**

Démonstration :

- .....
- .....
- .....
- .....
- .....

■

C - Écriture d'un entier

C.1 - À l'aide de la division euclidienne

Propriété 14 : Partition

Dans la division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{N}^*$, il y a b restes possibles : $0, 1, ..., b-1$. Ainsi :
Tout entier $a \in \mathbb{Z}$, s'écrit sous une, et une seule forme, des formes suivantes :

$$\begin{cases} bq \\ bq+1 \\ . \\ . \\ . \\ bq+b-1 \end{cases}$$

où q est le quotient dans la division euclidienne de a par b.

Démonstration :

Dans la division euclidienne de a par b on sait que :

$$a = bq + r, \quad \text{où } 0 \leq r < b$$

Ceci démontre bien le choix des b restes possibles, et les b formes de a donné dans l'accolade.
L'unicité de l'écriture de a vient de l'unicité du reste dans la division euclidienne de a par b. ■

À savoir faire 8 : Disjonction de cas

1. Montrer que pour tout entier naturel n l'entier $u_n = n(n+1)(2n+1)$ est divisible par 3.
   Soit $n \in \mathbb{N}$ en considérant son écriture dans la division euclidienne par 3 on sait qu'il existe $q \in \mathbb{N}$ tel que :

   $$n = 3q \quad \text{ou} \quad n = 3q+1 \quad \text{ou} \quad n = 3q+2$$

   Considérons les différents cas :

   - **$r = 0$**

     $$u_n = u_{3q} = 3q(3q+1)(6q+1) = 3 \times q(3q+1)(6q+1) \quad \text{où } q(3q+1)(6q+1) \in \mathbb{Z}$$

     D'où $3 \mid u_{3q}$.
   - **$r = 1$**

     $$u_n = u_{3q+1} = (3q+1)(3q+2)(6q+3) = 3 \times (3q+1)(3q+2)(2q+1) \quad \text{où } (3q+1)(3q+2)(2q+1) \in \mathbb{Z}$$

     D'où $3 \mid u_{3q+1}$.
   - **$r = 2$**

     $$u_n = u_{3q+2} = (3q+2)(3q+3)(6q+5) = 3 \times (3q+2)(q+1)(6q+5) \quad \text{où } (3q+2)(q+1)(6q+5) \in \mathbb{Z}$$

     D'où $3 \mid u_{3q+2}$.

   Ainsi par disjonction on en conclut que pour tout $n \in \mathbb{N}$, on a $3 \mid u_n$.
2. Montrer ensuite que cet entier est également divisible par 6.
   En conservant la disjonction de cas que l'on vient de faire on a :
   - **$r = 0$**

     $$u_{3q} = 3K \quad \text{où } K = q(3q+1)(6q+1) \in \mathbb{Z}$$

     En montrant que K est pair on aura alors $K = 2t$ où $t \in \mathbb{Z}$ d'où :

     $$u_{3q} = 3K = 3 \times 2t = 6t$$

     Étudions alors $K = q(3q+1)(6q+1)$:
     - Ou bien q est pair et on a déjà un facteur pair.
     - Ou bien q est impair et donc $3q+1$ est pair.

     Dans tous les cas on montre que l'un des facteurs de K est pair donc K est pair.
     D'où u_{3q} est un multiple de 6.
   - **$r = 1$**

     $$u_{3q+1} = 3 \times K \quad \text{où } K = (3q+1)(3q+2)(2q+1) \in \mathbb{Z}$$

     Étudions K, $3q+1$ et $3q+2$ sont deux entiers consécutifs donc l'un des deux est pair (peut importe la valeur de q). Ainsi, il existe toujours au moins un facteur pair dans K donc K est pair.
     D'où u_{3q+1} est un multiple de 6.

- **$r = 2$**

$$u_{3q+2} = 3 \times K \quad \text{où } K = (3q+2)(q+1)(6q+5) \in \mathbb{Z}$$

Étudions alors $K = (3q+2)(q+1)(6q+5)$:

- Ou bien q est pair et donc $3q+2$ est pair.
- Ou bien q est impair et donc $q+1$ est pair.

Dans tous les cas on montre que l'un des facteurs de K est pair donc K est pair.
D'où u_{3q+2} est un multiple de 6.

Par disjonction de cas on vient de montrer que pour tout $n \in \mathbb{N}$, on a u_n qui est divisible par 6.

Bonus : Pour ceux que ça amuse déterminer (on attend une preuve pas seulement une affirmation) par quel entier est divisible le nombre $n(n+1)(n+2)(n+3)$ pour tout $n \geq 1$.

Réponse : Pour tout $n \geq 1$, $24 \mid n(n+1)(n+2)(n+3)$

C.2 - Écriture d'un entier dans une base

Vous avez appris au collège que l'écriture que l'écriture usuelle des nombres est basée sur les puissances de 10, par exemple :

$$3724 = 3 \times 10^3 + 7 \times 10^2 + 2 \times 10^1 + 4 \times 10^0$$

Plus généralement, si on note $c_0, c_1, ..., c_N$ les chiffres de l'écriture de l'entier n (ici on remarque que notre entier n possède N dans son écriture) lus de droite à gauche, alors :

$$n = c_0 10^0 + c_1 10^1 + ... + c_N 10^N$$

On dira que :

$$n = \underline{c_N c_{N-1} ... c_1 c_0}_{10}$$

est l'écriture en base 10 du nombre n.
Bien sûr on peut chercher à donner l'écriture d'un entier dans une autre base :

Exemple :

- Écrire 5 en base 2, puis en base 3, puis en 5.
  ▶ On a : $5 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$, donc $5 = \underline{101}_2$
  ▶ On a : $5 = 1 \times 3^1 + 2 \times 3^0$, donc $5 = \underline{12}_3$
  ▶ On a : $5 = 1 \times 5^1 + 0 \times 5^0$, donc $5 = \underline{10}_5$
- Écrire 10 en base 2, puis en base 3, puis en 5.
  ▶ On a : $10 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$, donc $10 = \underline{1010}_2$
  ▶ On a : $10 = 1 \times 3^2 + 0 \times 3^1 + 1 \times 3^0$, donc $10 = \underline{101}_3$
  ▶ On a : $10 = 2 \times 5^1 + 0 \times 5^0$, donc $10 = \underline{20}_5$
- Écrire 25 en base 2, puis en base 3, puis en 5.
  ▶ On a : $25 = 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$, donc $25 = \underline{11001}_2$
  ▶ On a : $25 = 2 \times 3^2 + 2 \times 3^1 + 1 \times 3^0$, donc $25 = \underline{221}_3$
  ▶ On a : $25 = 1 \times 5^2 + 0 \times 5^1 + 0 \times 5^0$, donc $5 = \underline{100}_5$

Méthode 1 : Déterminer l'écriture d'un nombre donné en base 10 vers une autre base.

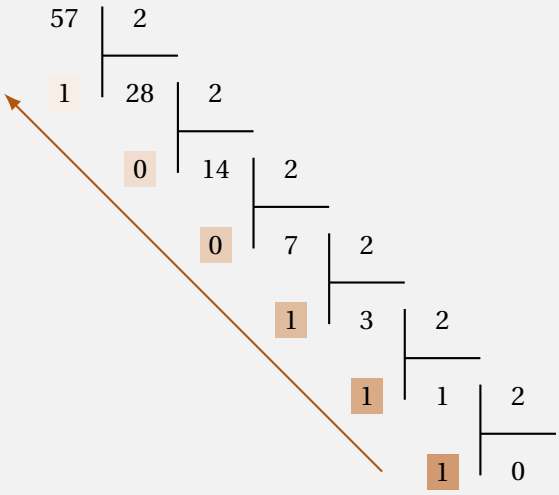
Soit N le nombre entier que l'on souhaite écrire vers la base $a \in \mathbb{N}$, la méthode à suivre est la suivante :

- **Étape 1 :** Effectuer la division euclidienne de N par a.
  ▷ On conserve le quotient ;
  ▷ Le **reste** correspond au chiffre le plus à droite du nombre dans la nouvelle base.
- **Étape 2 :** On effectue la division euclidienne du quotient par a.

▷ On conserve le nouveau quotient ;
▷ Le nouveau **reste** correspond au chiffre suivant du nombre dans la nouvelle base.

- **Étape 3 :** Continuer ainsi de suite tant que le quotient est supérieur ou égal à 1.
- **Étape 4 :** Quand le quotient devient nul, la conversion est terminée.
  ▷ Le dernier reste correspond au chiffre le plus à gauche du nombre dans la nouvelle base.

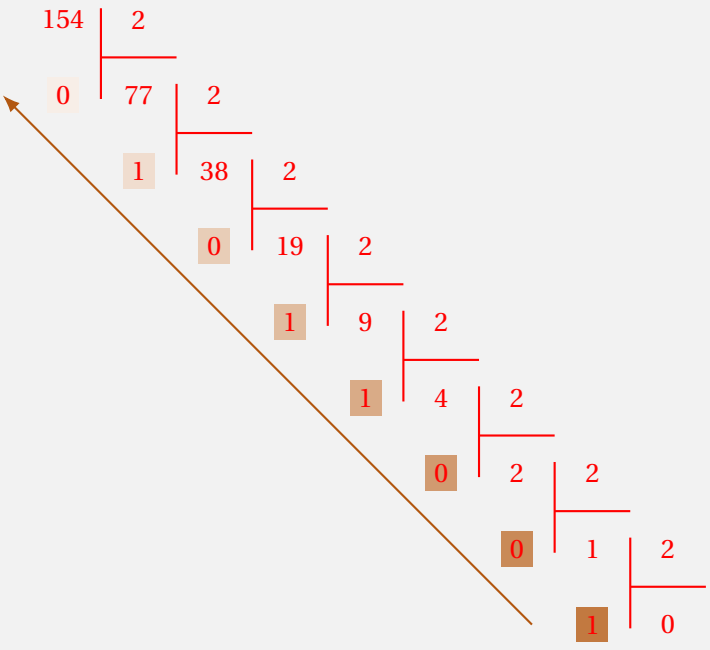
Voici cette méthode sur la détermination de l'écriture de 57 en base 2.



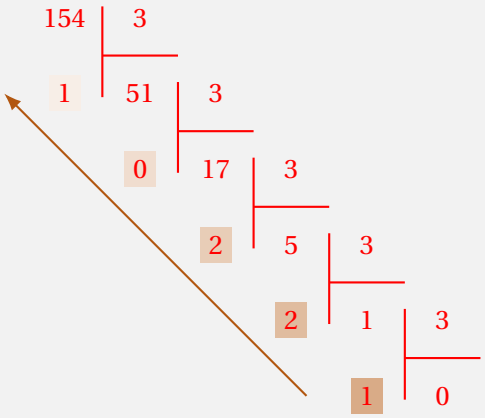
C'est-à-dire : $57 = \underline{111001}_2$.

À savoir faire 9 : Base 10 → Base a

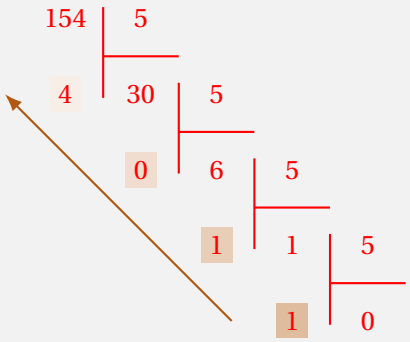
Déterminer l'écriture de 154 en base 2, puis base 3 et enfin base 5.



Ce qui nous donne $\underline{10011010}_2$

- 

  Ce qui nous donne $\underline{12201}_3$

- 

  Ce qui nous donne $\underline{1104}_5$

À savoir faire 10 : Base 10 ← Base a

À quel nombre (sous-entendu en base 10) sont égaux les nombres suivants :

- $\underline{11101}_2$
  On a $\underline{11101}_2 = 1\times2^0+0\times2^1+1\times2^2+1\times2^3+1\times2^4 = 1+4+8+16 = 29$
- $\underline{121}_3$
  On a $\underline{121}_3 = 1\times3^0+2\times3^1+1\times3^2 = 1+6+9 = 16$
- $\underline{4321}_5$
  On a $\underline{4321}_5 = 1\times5^0+2\times5^1+3\times5^2+3\times5^3+4\times5^4 = 1+10+75+3\times125+4\times625 = 86+375+2500 = 2961$

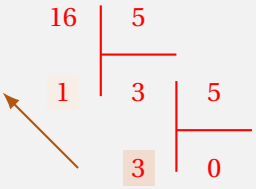
À savoir faire 11 : Base a → Base b

Donner en base 5 les nombres suivants :

- $\underline{121}_3$
  En utilisant le à savoir faire précédent on sait que :

  $$\underline{121}_3 = 16$$

  Il nous reste donc à donner l'écriture de 16 en base 5 :

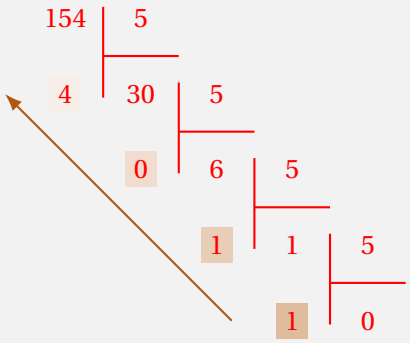
Donc :

$$\underline{121}_3 = \underline{31}_5$$

- $\underline{10011010}_2$ D'après le à savoir faire encore précédent on sait que :

$$\underline{10011010}_2 = 154$$

Il nous reste donc à donner l'écriture de 154 en base 5 :



Donc :

$$\underline{10011010}_2 = \underline{1104}_5$$

Théorème 6 : Changement de base

Soit $a \geq 2$ un entier et $k \in \mathbb{N}$.
Alors, pour tout $n \in \mathbb{N}$ tel que $a^k \leq n < a^{k+1}$, on peut trouver des entiers $c_0, c_1, ..., c_{k-1}, c_k \in [\![0, a-1]\!]$ tels que :

$$n = c_0 a^0 + c_1 a^1 + ... + c_{k-1} a^{k-1} + c_k a^k$$

De plus cette écriture est unique.
La suite des chiffres c_i est appelé représentation (ou écriture) en base a. On écrira :

$$n = \underline{c_k c_{k-1} ... c_0}_a$$

À retenir : Que nous dit ce théorème?
Concrètement il nous assure que l'on peut transformer tout entier dans une autre base a (différente de 1 étant donné qu'en base 1 tout nombre aura pour représentation 0, les restes sont toujours égaux à 0). De plus il nous assure que si $a^k \leq n < a^{k+1}$ alors n aura $k+1$ chiffres dans sa représentation.

Information : Les bases.
Les plus importantes sont l'écriture en base 10 (celle qu'on utilise tous les jours), l'écriture en base 2 (binaire) et l'écriture en base 16 (hexadécimale) très utilisées pour représenter les données dans la mémoire des ordinateurs.

Démonstration :
La démonstration se construit de la même manière que pour la détermination de l'écriture dans une base. Cherchons à écrire n en base a, pour cela effectuons les divisions euclidiennes successives par a jusqu'à obtenir 0 comme quotient.

- $n = aq_0 + r_0$ où (q_0, r_0) est un couple d'entiers naturels tels que $0 \leq r_0 < a$
- $q_0 = aq_1 + r_1$ où (q_1, r_1) est un couple d'entiers naturels tels que $0 \leq r_1 < a$
- $q_1 = aq_2 + r_2$ où (q_2, r_2) est un couple d'entiers naturels tels que $0 \leq r_2 < a$

- ...

Montrons que l'algorithme de division euclidienne successives par a va nous faire aboutir en un nombre fini d'étape à un quotient $q_k = 0$.
La suite des $(q_i)_i$ ainsi définie une suite d'entiers naturels strictement décroissante, en effet :

- Pour tout $i \in \mathbb{N}$, $q_i \in \mathbb{N}$ par définition de la division euclidienne car $a \in \mathbb{N}^*$ et $n \in \mathbb{N}$.
- Elle est strictement décroissante car pour $i \in \mathbb{N}$ on a :

$$q_i = aq_{i+1} + r_{i+1} \geq aq_{i+1}$$

car $r_{i+1} \geq 0$. Donc en ajoutant et retranchant q_{i+1} on a :

$$q_i \geq q_{i+1} + (a-1)q_{i+1}$$

Or on sait que $a \geq 2$ donc $(a-1)q_{i+1} > 0$. Donc :

$$q_i < q_{i+1}$$

D'où $(q_i)_i$ est une suite strictement décroissante.

Ainsi comme suite d'**entiers naturels** strictement décroissante il existe un rang $k \in \mathbb{N}$ tel que $q_k = 0$. On a alors :

$$q_{k-1} = a \times 0 + r_k \quad 0 \leq r_k < b$$

On pose alors $c_0 = r_0, c_1 = r_1, ..., c_k = r_k$ et dans ce cas on a :

- $q_{k-1} = a \times 0 + c_k$
- $q_{k-2} = a \times q_{k-1} + c_{k-1} = ac_k + c_{k-1}$
- $q_{k-3} = a \times q_{k-2} + c_{k-2} = a^2 c_k + ac_{k-1} + c_{k-2}$
- ...
- $n = aq_0 + r_0 = a^k c_k + a^{k-1} c_{k-1} + ... + a^1 c_1 + a^0 c_0$

L'unicité des coefficients $c_k, c_{k-1}, ..., c_1, c_0$ vient de l'unicité des restes dans les divisions euclidiennes successives, étant donné que pour tout $i \in [\![0, k]\!]$ on a :

$$c_i = r_i$$

D - Vers la congruence

Propriété 15 : Vers la définition de congruence

Pour tout $a \in \mathbb{Z}$, la division euclidienne par b permet d'associer un unique reste r.
Deux entiers a et a' ont alors même reste dans la division euclidienne par b si, et seulement si,

$$b \mid a - a'$$

Démonstration :

- L'unicité du reste est donné par le théorème de la division euclidienne.
- Soient $a, a' \in \mathbb{Z}$ et $b \in Z^*$,
  $\Rightarrow$ Supposons que a et a' ont le même reste dans la division euclidienne par b.
  Donc il existe $q, q' \in \mathbb{Z}$ et $r \in \mathbb{Z}$ tels que :

$$\begin{cases} a = bq + r, & \text{où } 0 \leq r < |b| \\ a' = bq' + r, & \text{où } 0 \leq r < |b| \end{cases}$$

Donc $a-a' = bq+r-bq'-r = b(q-q')$ d'où $b \mid a-a'$.
$\boxed{\Leftarrow}$ Supposons que $b \mid a-a'$, donc le reste dans la division euclidienne de $a-a'$ par b est égal à 0.
De plus on sait d'après le théorème de la division euclidienne qu'il existe deux unique couples d'entiers (q,r) et (q',r') tels que :

$$\begin{cases} a = bq+r, & \text{où } 0 \leq r < |b| \\ a' = bq'+r', & \text{où } 0 \leq r' < |b| \end{cases}$$

Deux cas possibles :

- Ou bien $0 \leq r' \leq r < |b|$ On a alors que

$$a-a' = b(q-q')+r-r'$$

Où $r-r' \geq 0$ et $r-r' < |b|$ donc $r-r'$ est le reste dans la division euclidienne de $a-a'$ par b, d'où par unicité du reste on a :

$$r-r' = 0 \Leftrightarrow r = r'$$

- Ou bien $0 \leq r \leq r' < |b|$ On a alors que

$$a'-a = b(q'-q)+r'-r$$

Où $r'-r \geq 0$ et $r'-r < |b|$ donc $r'-r$ est le reste dans la division euclidienne de $a'-a$ par b.
Or on sait que $b \mid a-a'$ donc $b \mid -(a-a')$ c'est-à-dire $b \mid a'-a$, ainsi le reste dans la division euclidienne de $a'-a$ par b est 0, d'où par unicité du reste on a :

$$r'-r = 0 \Leftrightarrow r = r'$$

■

Partie III Congruence

A - Définition

Définition 6 : Congru

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
On dit que a est congru b modulo n lorsque a ont le même reste dans la division euclidienne par n.
On notera alors :

$$a \equiv b[n] \quad \text{ou} \quad a \equiv b \bmod(n)$$

D'après la propriété qui précède directement cette définition on a alors :

Propriété 16 : Caractérisation d'une congruence

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on a :

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

De plus,

$$a \equiv b[n] \Leftrightarrow \exists k \in \mathbb{Z},\ a = b+kn$$

Démonstration :

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$,

D'après la propriété précédente on sait que :

$$n \mid a-b \Leftrightarrow a \text{ et } b \text{ ont même reste dans la division euclidienne par } n]$$

Par définition de la congruence on a alors :

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

Comme on a :

$$n \mid a-b \Leftrightarrow \exists k \in \mathbb{Z},\ a-b=kn \Leftrightarrow \exists k \in \mathbb{Z},\ a=b+kn$$

On a aussi :

$$a \equiv b[n] \Leftrightarrow \exists k \in \mathbb{Z},\ a=b+kn$$

■

Exemple :

On a $215 \equiv 7[16]$ en effet : on a $215-7=208$.
Or on sait que $16 \times 10 = 160$ de plus $208-160=48=16\times 3$ donc :

$$208 = 16 \times 13$$

À savoir faire 12 : Reste

Montrer que si r est le reste de la division euclidienne de $a \in \mathbb{Z}$ par $n \in \mathbb{N}^*$, alors :

$$a \equiv r[n]$$

D'après le théorème de la division euclidienne on sait qu'il existe $q \in \mathbb{Z}$ tel que :

$$a = nq + r, \quad \text{avec } 0 \leq r < n$$

D'où $a = r + nq$ avec $q \in \mathbb{Z}$ donc :

$$a \equiv r[n]$$

Propriété 17 : Divise

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on a :

$$a \equiv 0[n] \Leftrightarrow n \mid a$$

Démonstration :

C'est un cas particulier de la propriété précédente. ■

B - Propriétés - opérations

Propriété 18 : Relation de congruence

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$,

- *(Réflexivité)* $a \equiv a[n]$;
- *(Symétrie)* Si $a \equiv b[n]$ alors $b \equiv a[n]$;
- *(Transitivité)* Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$;

Démonstration :

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$

- Clairement on a : $n \mid a - a$ car $n \mid 0$ d'où $a \equiv a[n]$.
- Supposons que $a \equiv b[n]$ donc $n \mid a - b$. Comme on sait que si $a \mid b$ alors $a \mid -b$, donc ici :

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

- Supposons que $a \equiv b[n]$ et $b \equiv c[n]$, donc :

$$n \mid a - b \quad \text{et} \quad n \mid b - c$$

On a alors d'après une propriété de la relation divise :

$$n \mid a - b + b - c \Rightarrow n \mid a - c \Leftrightarrow a \equiv c[n]$$

■

Propriété 19 : Reste

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, on a :

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

Démonstration :

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$,

$\Rightarrow$ Voir À savoir faire 12.

$\Leftarrow$ Supposons que $a \equiv r[n]$ et $0 \leq r < n$.

Comme $a \equiv r[n]$ on sait que $\exists k \in \mathbb{Z}$, tel que :

$$a = r + nk = nk + r \quad \text{où } 0 \leq r < n$$

D'où d'après le théorème de la division euclidienne on a que le reste dans la division euclidienne de a par n est r. ■

Propriété 20 : Opérations

Soient $a, b, c, d, k_1, k_2 \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
Si $a \equiv b[n]$ et $c \equiv d[n]$ alors :

- ***(Somme)*** $a + c \equiv b + d[n]$;
- ***(Soustraction)*** $a - c \equiv b - d[n]$;
- ***(Produit)*** $ac \equiv bd[n]$;
- ***(Multiplication par un scalaire)*** $k_1 a \equiv k_1 b$;
- ***(Combinaison linéaire)*** $k_1 a + k_2 c \equiv k_1 b + k_2 d[n]$;
- ***(Passage à la puissance)*** Pour tout $k \in \mathbb{N}$, $a^k \equiv b^k[n]$

Démonstration :

Soient $a, b, c, d, k_1, k_2 \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.
Supposons que $a \equiv b[n]$ et $c \equiv d[n]$:

- **Somme :** On sait que :

$$n \mid a - b \quad \text{et} \quad n \mid c - d$$

Donc d'après une propriété de la relation divise on a alors :

$$n \mid a-b+c-d \Leftrightarrow n \mid a+c-(b+d) \Leftrightarrow a+c \equiv b+d[n]$$

- **Soustraction :** Si $c \equiv d[n]$ on a alors qu'il existe $k \in \mathbb{Z}$ tel que :

$$c = d + kn$$

On a alors également :

$$-c = -d - kn = -d + k'n \quad \text{où } k' = -k \in \mathbb{Z}$$

Donc : $-c \equiv -d[n]$. On a alors d'après la propriété précédente que :

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

- **Produit :** Par caractérisation de la congruence on a :

$$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Leftrightarrow \begin{cases} a = b + kn, & \text{avec } k \in \mathbb{Z} \\ c = d + k'n, & \text{avec } k' \in \mathbb{Z} \end{cases}$$

D'où :

$$\begin{aligned} ac &= (b+kn)(d+k'n) \\ &= bd + bk'n + dkn + kk'n^2 \\ &= bd + n\left(bk' + dk + kk'n\right) \\ &= bd + nK \end{aligned}$$

où $K = bk' + dk + kk'n \in \mathbb{Z}$, donc $ac \equiv bd[n]$.

- **Multiplication par un scalaire :** D'après le point précédent on a l'implication suivante :

$$\begin{cases} a \equiv b[n] \\ k_1 \equiv k_1[n] \end{cases} \Rightarrow ak_1 \equiv bk_1[n]$$

- **Combinaison linéaire :** En combinant les points **multiplication par un scalaire** et **somme** on a :

$$\begin{cases} k_1 a \equiv k_1 b[n] \\ k_2 c \equiv k_2 d[n] \end{cases} \Rightarrow k_1 a + k_2 c \equiv k_1 b + k_2 d[n]$$

- **Passage à la puissance :** Par récurrence, posons le prédicat (la propriété dépendant d'une variable, la valeur de vérité dépend de cette variable).

$$\forall k \in \mathbb{N},\ \mathscr{P}(k) : \text{« } a^k \equiv b^k[n] \text{ »}$$

► **Initialisation :** Pour $k = 0$
On a bien $a^0 \equiv b^0[n]$ car $1 \equiv 1[n]$ car $n \div 1 - 1$.
► **Hérédité :** Soit $k \in \mathbb{N}$, supposons que le prédicat $\mathscr{P}(k)$ est vraie au rang k, montrons qu'il est vraie au rang $k+1$.
Par hypothèse de récurrence on sait que : $a^k \equiv b^k[n]$, on a alors d'après le point **produit** :

$$\begin{cases} a^k \equiv b^k[n] \\ a \equiv b[n] \end{cases} \Rightarrow a^k a \equiv b^k b[n] \Leftrightarrow a^{k+1} \equiv b^{k+1}[n]$$

D'où on vient de montrer que $\mathscr{P}(k+1)$ est vraie.
► **Conclusion :** Le prédicat a été initialisé au rang $k = 0$, de plus il est héréditaire donc d'après le principe de récurrence on peut affirmer que $P(k)$ est vraie pour tout $k \in \mathbb{N}$.

À savoir faire 13 : Opérations

1. En dressant un certain tableau de congruence démontrer que $24 \mid n(n+1)(n+2)(n+3)$.
   À corriger
2. On cherche à savoir par quel chiffre se termine $12^{100}+45^{10}-13^{14}$
   (a) Déterminer le reste dans la division euclidienne par 10 de $12^k, 13^k$ et 45^k pour tout $k \in [\![1,5]\!]$.
   À corriger
   (b) En déduire un moyen de déterminer le reste dans la division euclidienne par 10 de $12^k, 13^k$ et 45^k pour tout $k \in \mathbb{Z}$.
   À corriger
   (c) Conclure.
   À corriger
3. Déterminer le reste de la division euclidienne de 2^{456} par 5.
   À corriger, il faut aller chercher à obtenir une puissance k tel que $2^k \equiv 1[5]$
4. Déterminer le reste de la division euclidienne de 23^{137} par 7.
   À corriger

Attention : La congruence n'est pas compatible avec la division.

Si $a \equiv b[n]$ nous n'avons pas $\frac{a}{k} \equiv \frac{b}{k}[n]$ (même si $k \mid a$ et b). En effet :

$$8 \equiv 12[4] \quad \textbf{mais} \quad 4 \not\equiv 6[4]$$

Voici l'une des propriétés qui peut se rapprocher d'une division :

Propriété 21 :

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, $q \in \mathbb{N}^*$ tel que $q \mid n$ on a alors :

$$a \equiv b[q]$$

Démonstration :

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, $q \in \mathbb{N}^*$ tel que $q \mid n$.
Supposons que $a \equiv b[n]$, on a alors :

$$\exists k \in \mathbb{Z},\ a = b + kn$$

Or on sait que $q \mid n$, donc :

$$\exists k' \in \mathbb{Z},\ n = k'q$$

D'où :

$$a = b + kk'q \quad \text{où } kk' \in \mathbb{Z}$$

Ainsi on a bien :

$$a \equiv b[q]$$

■

À savoir faire 14 : Appliquer la congruence à des situations du quotidien

1. Il est 7h, quelle heure sera-t-il dans 741h ?
   À corriger
2. Mon anniversaire tombe un samedi cette année, quel jour tombera-t-il l'année prochaine (en supposant que l'année en cours pas bissextile) ?
   À corriger
3. Ma cousine est née un 29 février et fête son anniversaire tous les quatre ans. En 2024 c'était un samedi,

quel jour tombera son anniversaire en 2024 ?
À corriger

C - Équations

À savoir faire 15 : Savoir résoudre dans $\mathbb{Z}$ une équation du premier ordre modulo n

1. Déterminer l'ensemble des entiers x tels que : $6x+2 \equiv 5x+1[3]$.
   On a :
$$\begin{aligned} & 6x+2 \equiv 5x+1[3] \\ \Leftrightarrow\ & x+2 \equiv 1[3] \\ \Leftrightarrow\ & x \equiv -1[3] \\ \Leftrightarrow\ & x \equiv 2[3] \end{aligned}$$
   Ainsi $\mathscr{S} = \{3k+2 \ / \ k \in \mathbb{Z}\}$
2. Déterminer l'ensemble des entiers x tels que : $2x \equiv 1[7]$.
   Attention nous n'avons pas le droit de diviser par 2 !
   On établit alors le tableau de congruence modulo 7 de x et $2x$. On remarque alors que seul $x \equiv 4[7]$ nous assure $2x \equiv 1[7]$. Donc :
$$\mathscr{S} = \{7k+4 \ / \ k \in \mathbb{Z}\}$$
3. Déterminer l'ensemble des entiers x tels que : $5x+2 \equiv 2x+9[8]$. On a :
$$\begin{aligned} & 5x+2 \equiv 2x+9[8] \\ \Leftrightarrow\ & 3x \equiv 7[8] \end{aligned}$$
   On établit alors le tableau de congruence modulo 8 de x et $3x$. On remarque alors que seul $x \equiv 5[8]$ nous assure $3x \equiv 7[8]$. Donc :
$$\mathscr{S} = \{8k+5 \ / \ k \in \mathbb{Z}\}$$

D - Critères de divisibilité

Propriété 22 : Critères de divisibilité

Un entier n est :

- **divisible par 2** si, et seulement si, son chiffre des unités est $0, 2, 4, 6$ ou 8.
- **divisible par 3** si, et seulement si, la somme de ses chiffres est divisible par 3.
- **divisible par 4** si, et seulement si, le nombre formé par ses deux derniers chiffres est divisible par 4.
- **divisible par 5** si, et seulement si, son chiffre des unités est 0 ou 5.
- **divisible par 6** si, et seulement si, il est divisible par 2 **et** 3.
- **divisible par 7** si, et seulement si, la différence entre le nombre de dizaines de n et le double du chiffre des unités est divisible par 7.
- **divisible par 8** si, et seulement si, le nombre formé par ses trois derniers chiffres est divisible par 8.
- **divisible par 9** si, et seulement si, la somme de ses chiffres est divisible par 9.
- **divisible par 10** si, et seulement si, son chiffre des unités est 0.

- **divisible par 11** si, et seulement si, la différence entre la somme des chiffres en position impaire (unité, centaine,...) et la somme des chiffres en position paire (dizaine, millier,...) est divisible par 11.

À savoir faire 16 : Critères de divisibilité

Compléter le tableau à l'aide de `OUI` ou `NON` ou `NSP` (ne sait pas)

... est divisible par ...?	2	3	4	5	6	7	8	9	10	11
123456										
975310										
9555										
8127453276										
111222333444555666777888										
16478										
392712156114										
1397										
72039										
6017										

Démonstration :

Soit $n \in \mathbb{Z}$, l'idée est de donner l'écriture en base 10. Notons la :

$$n = \underline{a_q a_{q-1} ... a_1 a_0}_{10}$$

C'est-à-dire :

$$n = a_q 10^q + a_{q-1} 10^{q-1} + ... a_1 10 + a_0$$

- **Divisible par 2** : On sait que :

$$2 \mid n \Leftrightarrow n \equiv 0[2]$$

Or comme pour tout $k \in \mathbb{N}^*$, on a $10^k \equiv 0[2]$, ainsi d'après les propriétés de la congruence on a :

$$n = a_q 10^q + a_{q-1} 10^{q-1} + ... a_1 10 + a_0 \equiv a_q \times 0 + a_{q-1} \times 0 + ... + a_1 \times 0 + a_0 [2]$$

C'est-à-dire :

$$n \equiv a_0 [2]$$

Donc :

$$2 \mid n \Leftrightarrow a_0 \equiv 0[2]$$

C'est-à-dire, n est divisible par 2 si, et seulement si, son chiffre des unités est divisible 2.
Comme $a_0 \in [\![0,9]\!]$, on a a_0 est divisible par 2 si, et seulement si, $a_0 \in \{0,2,4,6,8\}$.
Ainsi :

$$n \text{ est divisible par } 2 \Leftrightarrow a_0 \in \{0,2,4,6,8\}$$

- **Divisible par 5** : On raisonne de la même manière que pour 2 car :

$$\forall k \in \mathbb{N}^*,\ 10^k \equiv 0[5]$$

On a alors

$$n \equiv a_0[5]$$

Donc :

$$5 \mid n \Leftrightarrow a_0 \equiv 0[5]$$

C'est-à-dire, n est divisible par 5 si, et seulement si, son chiffre des unités est divisible 5, dans ce cas on a si, et seulement si, $a_0 \in \{0,5\}$.
Ainsi :

$$n \text{ est divisible par } 5 \Leftrightarrow a_0 \in \{0,5\}$$

- **Divisible par 10** : Idem pour 10, car on a évidemment :

$$\forall k \in \mathbb{N}^*,\ n \equiv a_0[10]$$

Donc $10 \mid n$ si, et seulement $10 \mid a_0$ et comme a_0 est comprit entre 0 et 9 on a :

$$10 \mid a_0 \Leftrightarrow a_0 = 0$$

D'où n est divisible par 10 si, et seulement si, son chiffre des unités est 0.

- **Divisible par 3** : On sait que :

$$3 \mid n \Leftrightarrow n \equiv 0[3]$$

Or comme, $10 \equiv 1[3]$ on a pour tout $k \in \mathbb{N}$, on a $10^k \equiv 1[3]$, ainsi d'après les propriétés de la congruence on a :

$$n = a_q 10^q + a_{q-1}10^{q-1} + ...a_1 10 + a_0 \equiv a_q \times 1 + a_{q-1} \times 1 + ... + a_1 \times 1 + a_0[3]$$

C'est-à-dire :

$$n \equiv a_q + a_{q-1} + ... + a_1 + a_0[3]$$

Donc :

$$2 \mid n \Leftrightarrow a_q + a_{q-1} + ... + a_1 + a_0 \equiv 0[3]$$

C'est-à-dire, n est divisible par 3 si, et seulement si, la somme de ses chiffre est divisible 3.

- **Divisible par 9** : On démontre le critère de divisibilité par 9 de la même manière car :

$$10 \equiv 1[9]$$

- **Divisible par 4** : On sait que :

$$4 \mid n \Leftrightarrow n \equiv 0[4]$$

Or on sait que pour $k \geq 2$ on a $10^k = 10^2 \times 10^{k-2} = 4 \times 25 \times 10^{k-2}$. Donc pour tout $k \geq 2$ on a :

$$10^k \equiv 0[4]$$

Donc on a :

$$n = a_q 10^q + a_{q-1}10^{q-1} + ... + a_2 10^2 + a_1 10 + a_0 \equiv a_1 10 + a_0[4]$$

On a alors :

$$4 \mid n \Leftrightarrow \underline{a_1 a_0}_{10} \equiv 0[4]$$

On vient alors de démontrer que n est divisible par 4 si, et seulement si, le nombre formé par ses deux derniers chiffres $\left(\underline{a_1 a_0}_{10}\right)$ est divisible par 4.

- **Divisible par 8** : On démontre de la même manière pour 8,
  Car on sait que pour $k \geq 3$ on a :

$$10^k = 10^3 \times 10^{k-3} = 10^2 \times 10 \times 10^{k-3} = 4 \times 25 \times 2 \times 5 \times 10^{k-3} = 8 \times 125 \times 10^{k-3}$$

  Donc pour tout $k \geq 3$ on a :

$$10^k \equiv 0[8]$$

  Donc on a :

$$n = a_q 10^q + a_{q-1} 10^{q-1} + ... + a_2 10^2 + a_1 10 + a_0 \equiv a_2 10^2 + a_1 10 + a_0 [8]$$

  On a alors :

$$8 \mid n \Leftrightarrow \underline{a_2 a_1 a_0}_{10} \equiv 0[8]$$

  On vient alors de démontrer que n est divisible par 8 si, et seulement si, le nombre formé par ses trois derniers chiffres $\left(\underline{a_2 a_1 a_0}_{10}\right)$ est divisible par 8.
- **Divisible par 6** : Malheureusement il nous manque quelques résultats d'arithmétiques pour pouvoir démontrer ce critère... Nous le pourrons au prochain chapitre.
- **Divisible par 11** : On sait que :

$$11 \mid n \Leftrightarrow n \equiv 0[11]$$

  Or on peut remarquer que :

$$\begin{cases} 10^0 \equiv 1[11] \\ 10^1 \equiv -1[11] \\ 10^2 = 99 + 1 \equiv 1[11] \end{cases}$$

  Ainsi pour tout entier k on a :

$$\begin{cases} 10^{2k} = \left(10^2\right)^k \equiv 1^k[11] \\ 10^{2k+1} = \left(10^2\right)^k \times 10 \equiv 1^k \times -1[11] \end{cases} \Leftrightarrow \begin{cases} 10^{2k} \equiv 1[11] \\ 10^{2k+1} \equiv -1[11] \end{cases}$$

  On vient alors de démontrer que toute puissance paire de 10 est congru à 1 modulo 11 et que toute puissance impaire de 10 est congru à -1 modulo 11.
  Ainsi suivant la parité de q on a :

$$n \equiv a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + ... + \pm a_q [11] \Leftrightarrow n \equiv (a_0 + a_2 + ...) - (a_1 + a_3 + a_5 + ...)\,[11]$$

  On vient de démontrer que n est congru à la différence entre la somme des chiffres en position impaire (en effet a_0 est en position 1, a_2 en position 3...) et la somme des chiffres en position paire (en effet a_1 est en position 2...).
  Donc :

$$11 \mid n \Leftrightarrow (a_0 + a_2 + ...) - (a_1 + a_3 + a_5 + ...) \equiv 0[11]$$

  C'est-à-dire :

  n est divisible par 11 $\Leftrightarrow$ la différence entre la somme des chiffres en position impaire et la somme des chiffres en position paire est divisible par 11

- **Divisible par 7** : Malheureusement comme pour 6 il nous manque des résultats pour pouvoir le justifier clairement.
  Une idée est :

$$n = 10k + r$$

  où k est le nombre de dizaine de n et r le chiffre des unités de n. On a alors :

$$\begin{aligned} 7 \mid n &\Leftrightarrow n \equiv 0[7] \\ &\Leftrightarrow 10q + r \equiv 0[7] \end{aligned}$$

Or comme $10q+r \equiv 3q+r[7]$ on a :

$$\begin{aligned} n \equiv 0[7] &\Leftrightarrow 3q+r \equiv 0[7] \\ &\Leftrightarrow 5(3q+r) \equiv 0[7] \\ &\Leftrightarrow 15q+5r \equiv 0[7] \\ &\Leftrightarrow q-2r \equiv 0[7] \end{aligned}$$

On vient alors de démontrer que n est divisible par 7 si, et seulement si, la différence entre le nombre de dizaine de n et le double des unités est divisible par 7.
L'équivalence marquée en rouge est le point clé du raisonnement, et jusqu'ici nous n'avons pas le droit de l'appliquer. En effet la propriété sur les opérations avec les congruences nous donne uniquement une implication et nous une équivalence :

$$A \equiv B[n] \Rightarrow cA \equiv cB[n]$$

L'autre sens dépend de notion (premier entre eux) que l'on a pas vu.
Puis l'idée de multiplier par 5 est un peu sorti du chapeau... il faudrait l'expliquer

■

Partie IV Vers le sup'

A - Relation de congruence

En prenant un peu de recul sur ce chapitre riche, nous constatons que la relation de congruence nous a permis de regrouper les nombres par paquets, chacun d'entre eux vérifiant une propriété particulière.

Exemple :

Modulo 2 : les nombres entiers sont regroupés en deux ensembles disjoints :

Les nombres **pairs** : ...;-4;-2;0;2;4;... et les nombres **impairs** : ...;-3;-1;1;3;5;...

Le premier de ces ensembles regroupent les nombres entiers ayant comme reste 0 dans la division euclidienne par 2.
Le second lui regroupent les nombres entiers ayant comme reste 1.
En pratique, modulo 2, nous ne faisons aucune différence entre les nombres 0;2;4;... (de même pour les nombres 1;3;5;...). Ainsi pour simplifier les calculs nous travaillons plutôt avec l'un d'entre eux (on choisira le plus simple) qui fait office de **représentant**. C'est-à-dire :

- $\overline{0}$ représente tous les nombres pairs ;
- $\overline{1}$ représente tous les nombres impairs.

Information : Fraction et représentant
Cette notion de représentant ne vous ait pas totalement étrangère. En effet, pour les fractions nous savons que :

$$\frac{1}{2} = \frac{2}{4} = \frac{-3}{-6} = \ldots$$

Ici $\frac{1}{2}$ est le représentant des fractions ayant comme développement décimal : 0,5.
Dans ce cas, on dit que l'on met en **relation** deux fractions, c'est-à-dire nous identifions deux fractions $\frac{a}{b}$ et $\frac{c}{d}$ si, et seulement si,

$$ad = bc$$

Exemple :

- On peut imaginer une situation hors des mathématiques, par exemple on peut créer une relation suivant la nationalité. On dirait alors qu'un $\texttt{individu}_1$ est en relation avec un $\texttt{individu}_2$ si, et seulement si, ils ont la même nationalité. Si on note $\sim$ cette relation on écrirait :

$$\texttt{individu}_1 \sim \texttt{individu}_2$$

- « Aimer » est une relation, si on note $\mathscr{R}$ la relation « aimer », on noterait : $\texttt{individu}_1$ est en relation avec $\texttt{individu}_2$ par :

$$\texttt{individu}_1 \mathscr{R} \texttt{individu}_2$$

Certaines relations ont des propriétés intéressantes qui vont nous permettre de définir des propriétés intéressante.

Définition 7 : Relation d'équivalence

Soit E un ensemble non vide, nous dirons que $\mathscr{R}$ est une **relation d'équivalence** sur l'ensemble des couples de l'ensemble E, que l'on notera $E \times E$, si $\mathscr{R}$ vérifie :

- *(Réflexivité)* Pour tout $x \in E$, $x \mathscr{R} x$;
- *(Symétrie)* Pour tout $x, y \in E$ tels que si $x \mathscr{R} y$ alors $y \mathscr{R} x$;
- *(Transitivité)* Pour tout $x, y, z \in E$ tels que si $x \mathscr{R} y$ et $y \mathscr{R} z$ alors $x \mathscr{R} z$;

Exemple :

- La relation de nationalité que l'on a définie précédemment (si on impose à chaque individu de n'avoir qu'une seule nationalité), est bien une relation d'équivalence en effet :
  - Elle est transitive tout individu est en relation avec lui même, étant donné qu'il a la même nationalité que lui même ;
  - Elle est symétrique, si vous êtes en relation avec votre voisin, c'est-à-dire que vous avez la même nationalité que lui alors lui aussi peut dire qu'il a la même nationalité que vous donc il est en relation avec vous ;
  - Elle est transitive, si vous avez la même nationalité qu'un $\texttt{individu}_2$ et que cet $\texttt{individu}_2$ a la même nationalité qu'un $\texttt{individu}_3$ alors vous avez la même nationalité que l'$\texttt{individu}_3$
    La transitivité n'est pas vérifiée si on laissait la possibilité d'avoir deux nationalité, car si on considère un `individu` français et espagnol alors on pourrait mettre en relation un français avec un espagnol.
- A contrario la relation « aimer » n'est pas une relation d'équivalence en effet :
  - Elle n'est pas transitive, certaines personnes ne s'aime pas ;
  - Elle n'est pas symétrique, si vous aimez quelqu'un parfois il peut arriver qu'elle ne vous aime pas en retour ;
  - Et elle n'est pas transitive car parfois vous pouvez aimer votre conjoint, que votre conjoint aime sa mère et que vous vous n'aimiez pas votre belle-mère (ceci n'est rien d'autre qu'un exemple...)
- La relation de congruence modulo n (un entier strictement supérieur à 1) est une relation d'équivalence en effet, on a vu qu'elle était réflexive, symétrique et transitive.

À partir d'une relation équivalence on peut alors définir :

Définition 8 : Classe d'équivalence

Soit E un ensemble non vide, muni d'une relation d'équivalence $\mathscr{R}$.
On appelle **classe d'équivalence** de $x \in E$ l'ensemble des éléments de E en relation avec x. C'est-à-dire :

$$\overline{x} = \{y \in E \ / \ x \mathscr{R} y\}$$

Nous dirons que $\overline{x}$ est le **représentant** de la classe d'équivalence.

Exemple :

- Pour la relation d'équivalence de nationalité, l'ensemble des français est une classe d'équivalence, l'ensemble des espagnols en est une autre. Dans la classe d'équivalence des Français on peut dire que l'on change de représentant tous les cinq ans.
- Dans l'exemple de notre chapitre, on définit la relation de congruence modulo n (un entier strictement supérieur à 1) pour deux entiers x, y par :

$$x \mathscr{R} y \Leftrightarrow x \equiv y[n]$$

En notant r le reste dans la division euclidienne de x par n, on sait que :

$$\begin{cases} 0 \leq r \leq n-1 \\ x \equiv r[n] \end{cases}$$

Par transitivité on a alors, pour tout $y \in \mathbb{Z}$ tel que :

$$y \mathscr{R} x \Leftrightarrow y \mathscr{R} r \Leftrightarrow y \equiv r[n]$$

C'est-à-dire : y est en relation avec x si, et seulement si, y a comme reste r dans la division euclidienne par n.
Donc la classe d'équivalence de x est :

$$\overline{x} = \{y \in \mathbb{Z} \ / \ x \mathscr{R} y\} = \{y \in \mathbb{Z} \ / \ y \equiv r[n]\}$$

La classe d'équivalence de x pour cette relation d'équivalence est l'ensemble des entiers ayant même reste dans la division euclidienne par n, on choisira généralement ce fameux reste comme représentant de la classe. Ici :

$$\overline{x} = \overline{r}$$

Ceci montre que les seules classes d'équivalences possible pour le relation d'équivalence de congruence modulo n correspondent aux seuls restes possibles dans la division euclidienne par n, c'est-à-dire :

$$\overline{0}, \overline{1}, ..., \overline{n-1}$$

L'unicité du reste, nous permet de passer des congruences dans $\mathbb{Z}$ à des égalités dans un nouvel ensemble... $\mathbb{Z}/n\mathbb{Z}$

B - $\mathbb{Z}/n\mathbb{Z}$

Définition 9 : $\mathbb{Z}/n\mathbb{Z}$

On note par $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation d'équivalence de congruence modulo n. On a alors :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ...\overline{n-1}\}$$

Grâce à toutes les propriétés de congruence modulo n, on peut définir les opérations suivantes :

Définition 10 : Opérations

Soit $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, on a alors :

- $\overline{a} + \overline{b} := \overline{a+b}$
- $\overline{a} - \overline{b} := \overline{a-b}$
- $\overline{a} \times \overline{b} := \overline{a \times b}$

Démonstration :

Soit $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, démontrons que ces opérations sont bien définis c'est-à-dire qu'elles ne dépendent pas du représentant choisi.
Pour être plus clair pour avoir des opérations consistantes, (prenons le cas de l'addition) il ne faudrait surtout pas que si l'on choisit des entiers a, a', b, b' tels que : $\overline{a'} = \overline{a}$ et $\overline{b'} = \overline{b}$ alors :

$$\overline{a'} + \overline{b'} \neq \overline{a} + \overline{b}$$

Cela voudrait dire que l'opération dépend du représentant choisit...

- Soient $a, a', b, b' \in \mathbb{Z}$ tels que : $\begin{cases} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{cases}$ on a alors : $\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases}$, donc il existe des entiers k, t tels que : $\begin{cases} a' = a + kn \\ b' = b + tn \end{cases}$ donc : $a' + b' = a + kn + b + tn = (a+b) + (k+t)n$ avec $k + t \in \mathbb{Z}$.
  Ainsi :
  $$a' + b' \equiv a + b[n]$$
  C'est-à-dire :
  $$\overline{a' + b'} = \overline{a+b}$$
  Alors on a bien :
  $$\overline{a'} + \overline{b'} = \overline{a} + \overline{b}$$
  L'opération d'addition ne dépend pas du représentant choisit.
- Soient $a, a', b, b' \in \mathbb{Z}$ tels que : $\begin{cases} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{cases}$ on a alors : $\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases}$, donc il existe des entiers k, t tels que : $\begin{cases} a' = a + kn \\ b' = b + tn \end{cases}$ donc : $a' - b' = a + kn - b - tn = (a-b) + (k-t)n$ avec $k - t \in \mathbb{Z}$.
  Ainsi :
  $$a' - b' \equiv a - b[n]$$
  C'est-à-dire :
  $$\overline{a' - b'} = \overline{a-b}$$
  Alors on a bien :
  $$\overline{a'} - \overline{b'} = \overline{a} - \overline{b}$$
  L'opération de soustraction ne dépend pas du représentant choisit.
- Soient $a, a', b, b' \in \mathbb{Z}$ tels que : $\begin{cases} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{cases}$ on a alors : $\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases}$, donc il existe des entiers k, t tels que : $\begin{cases} a' = a + kn \\ b' = b + tn \end{cases}$ donc : $a' \times b' = (a+kn)(b+tn) = ab + atn + bkn + ktn^2 = ab + (at + bk + ktn)n$ avec $at + bk + ktn \in \mathbb{Z}$.
  Ainsi :
  $$a' \times b' \equiv a \times b[n]$$
  C'est-à-dire :
  $$\overline{a' \times b'} = \overline{a \times b}$$

Alors on a bien :

$$\overline{a'} \times \overline{b'} = \overline{a} \times \overline{b}$$

L'opération de multiplication ne dépend pas du représentant choisit.

Les opérations ainsi définis sont consistantes. ■

À retenir : Calculer dans $\mathbb{Z}/n\mathbb{Z}$

Calculer dans $\mathbb{Z}/n\mathbb{Z}$, c'est calculer sur les entiers puis remplacer le résultat par le reste modulo n.

Exemple :

Concrètement pour calculer dans $\mathbb{Z}/12\mathbb{Z}$:

- $\overline{7}+\overline{8} = \overline{7+8} = \overline{15} = \overline{3}$ car $15 = 12\times 1+3$;
- $\overline{7}\times\overline{8} = \overline{7\times 8} = \overline{56} = \overline{8}$ car $56 = 12\times 4+8$.

Attention : En gardant le point de vue des nombres réels à partir de l'égalité :

$$\overline{7}\times\overline{8} = \overline{8}$$

On peut avoir très envie de « simplifier » par $\overline{8}$ de part et d'autre et d'obtenir : $\overline{7} = \overline{1}$ ce qui est bien évidemment **faux**!
En effet cette simplification vient de la division qui n'a pas été définie sur notre nouvel ensemble $\mathbb{Z}/12\mathbb{Z}$ (et plus généralement $\mathbb{Z}/n\mathbb{Z}$).

À savoir faire 17 : Tables

Dresser les tables de multiplication et d'addition dans $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

À savoir faire 18 : Intégrité?

Montrer que si n n'est pas premier, il existe $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ différents de $\overline{0}$ tels que $\overline{a}\times\overline{b} = \overline{0}$.
*Dans ce cas, on dira que $\mathbb{Z}/n\mathbb{Z}$ n'est pas **intègre**.*

.....

Propriété 23 : Règles

Soient $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/n\mathbb{Z}$ et $k, t \in \mathbb{N}$, on a :

- $\left(\overline{a}+\overline{b}\right)+\overline{c}=\overline{a}+\left(\overline{b}+\overline{c}\right)$
- $\overline{a}+\overline{b}=\overline{b}+\overline{a}$
- $\overline{a}+\overline{0}=\overline{a}$
- $\left(\overline{a}+\overline{b}\right)-\overline{a}=\overline{b}$
- $\left(\overline{a}\times\overline{b}\right)\times\overline{c}=\overline{a}\times\left(\overline{b}\times\overline{c}\right)$
- $\overline{a}\times\overline{b}=\overline{b}\times\overline{a}$
- $\overline{a}\times\overline{0}=\overline{0}$
- $\overline{a}\times\overline{1}=\overline{a}$
- $\overline{a}\times\left(\overline{b}+\overline{c}\right)=\overline{a}\times\overline{b}+\overline{a}\times\overline{c}$
- $\overline{a}^k\overline{a}^t=\overline{a}^{k+t}$
- $\overline{a}^k\overline{b}^k=\left(\overline{a}\overline{b}\right)^k$
- $\left(\overline{a}^k\right)^t=\overline{a}^{kt}$

Démonstration :

La démonstration est laissé en exercice :

■

À savoir faire 19 : L'identité remarquable de vos rêves

Donner dans $\mathbb{Z}/2\mathbb{Z}$ l'identité $\left(\overline{a}+\overline{b}\right)^2$.

Pour finir, on remarquera que le caractère fini de $\mathbb{Z}/n\mathbb{Z}$ (à contrario de $\mathbb{R}$ ou $\mathbb{Z}$) nous permet, quand n n'est pas trop grand, de résoudre des équations par force brute.

À savoir faire 20 : Équations

Résoudre dans $\mathbb{Z}/16\mathbb{Z}$ les équations :

- $\overline{2}\overline{x}+\overline{3}=\overline{4}$
- $\overline{x}^2+\overline{3}\overline{x}=\overline{x}-\overline{1}$

Partie V Exercices

A - Divisibilité

★½☆☆☆ **Exercice 1** (Liste des diviseurs)

1. Dresser la liste des diviseurs positifs des entiers 24, 49 et 126.
2. Et maintenant la liste des diviseurs de ces entiers.

★★½☆☆ **Exercice 2** (Aire)

Un terrain rectangulaire a des dimensions en mètres qui sont des entiers.
Déterminer ses dimensions sachant que sa largeur est un multiple de 3, que sa longueur est impaire et que son aire est de 300m^2.

★★½☆☆ **Exercice 3** (Cumuler les rôles)

Existe-t-il un entier qui soit multiple de 14 et diviseur de 100?

★★★☆☆ **Exercice 4** (Multiple)

Montrer que si n est un entier pair alors $n(n^2+20)$ est un multiple de 8.

★★☆☆☆ **Exercice 5** (Nombre de multiple)

1. Déterminer le nombre de multiples de 17 compris entre 2000 et 3000.
2. Déterminer le nombre de multiples de 41 compris entre -1000 et 2000.

★★½☆☆ **Exercice 6** (Récurrences)

1. Montrer, par récurrence, que pour tout entier $n \geq 1$,
$$17 \mid 3\times 5^{2n-1}+2^{3n-2}$$
2. Montrer, par récurrence, que pour tout entier naturel n,
$$7 \mid 4^{2n}-2^n$$

★★★☆☆ **Exercice 7** (Identité)

Soient $a, b \in \mathbb{Z}$, démontrer que :
$$3 \mid (a+b)^3 \Leftrightarrow 3 \mid a^3+b^3$$

★★★½☆ **Exercice 8** (Équations)

1. Déterminer les entiers n tels que $n+2 \mid n^3-2$
2. Résoudre l'équation $3xy-y^2=25$ d'inconnues entières x, y.
3. Résoudre l'équation $x^2=9y^2+7$ d'inconnues entières x, y.
4. Après avoir développé $(x+2)(y+1)$, résoudre l'équation $xy+x+2y=20$ d'inconnues entières x, y.

★★★☆☆ **Exercice 9** (Degré 3)

1. Montrer que si l'entier a est solution de l'équation $(E): x^3+x^2+bx+c=0$ où $b, c \in \mathbb{Z}$ alors a divise c.
2. L'équation $x^3+3x+3=0$ possède-t-elle des solutions entières?
3. Et l'équation $x^3-15x+4=0$?

★★★★☆ **Exercice 10** (Divisibilité par 5)

Pour $n \in \mathbb{N}$, notons $N_n = 1\underbrace{00...00}_{n \text{ zéros}}4^4 - \underbrace{9999...999}_{n+1 \text{ chiffres } 9}{}^4$.
Démontrer que, pour tout $n \in \mathbb{N}$, N_n est divisible par 5.

★★★☆☆ **Exercice 11** (Un avis ?)

Soient $p \in \mathbb{N}$ et $n \in \mathbb{Z}$ tels que :

$$p \mid n \quad \text{et} - p < n < p$$

Que peut-on dire de n ?

★★★½☆ **Exercice 12** (Divisibilité)

Démontrer que pour tout $n \in \mathbb{N}^*$, $3^{2n} - 2^n$ est divisible par 7.

B - Division euclidienne

★½☆☆☆ **Exercice 13** (À la tâche)

Effectuerla division euclidienne de a par b dans les cas suivants :

1. $a = 5689$; $b = 7$;
2. $a = 7$; $b = 5689$;
3. $a = -5689$; $b = 7$;
4. $a = 5689$; $b = -7$;

★☆☆☆☆ **Exercice 14** (Regrouper)

Soient a et b deux entiers naturels non nuls.
Regrouper les phrases ayant la même signification :

1. a est un diviseur de b;
2. a est divisible par b;
3. a est un multiple de b;
4. a divise b;
5. Le reste de la division euclidienne de a par b est 0;
6. Le quotient $\dfrac{a}{b}$ est un entier.

★★½☆☆ **Exercice 15** (À retrouver)

1. Déterminer tous les entiers naturels qui divisés par 7 renvoient un quotient égal au reste.
2. La différence entre deux entiers naturels a et b est égale à 779 et la division euclidienne de a par b donne 11 pour quotient et 49 comme reste.
   Déterminer a et b.

★★½☆☆ **Exercice 16** (Diviseur, quotient et reste)

1. La division eucldienne de 523 par un entier naturel non nul d a un quotient égal 17. Déterminer les valeurs possibles de d et du reste r.
2. La division euclidienne de 256 par un entier naturel b a un reste égal 25. Déterminer les valeurs possibles de b et du quotient q.

★★★½☆ **Exercice 17** (Carré et division euclidienne) .....

Démontrer que le carré de tout entier relatif est soit divisible par 3 soit donne 1 pour reste dans sa division euclidienne par 3

★★★★☆ **Exercice 18** (Une histoire de fourmi) .....

Une fourmi circule sur un anneau sur lequel sont placés dans l'ordre et dans le sens du parcours 8 points $A_0, A_1, ...A_7$. Elle part de A_0 et elle met 10 minutes pour aller d'un point à un autre. Après 5h40 de parcourt où se trouve-t-elle?

C - Congruence

★½☆☆☆ **Exercice 19** (Pour débuter) .....

Dans chacun des cas suivants, déterminer une valeur de a qui vérifient les conditions souhaitées :

1. $a \equiv -6[3]$ et $0 \leq a < 3$;
2. $a \equiv 57[11]$ et $0 \leq a < 11$;
3. $a \equiv 283[7]$ et $-5 < a \leq 2$;
4. $a \equiv -512[5]$ et $65 \leq a < 70$;
5. $a \equiv -12[10]$ et $35 \leq a < 45$;
6. $a \equiv 19[3]$ et $-10 < a \leq -7$.

★★☆☆☆ **Exercice 20** (Reste) .....

1. On suppose que : $\begin{cases} a \equiv 3[5] \\ b \equiv 4[5] \end{cases}$. Déterminer le reste de la division euclidienne de $7a^2 + 4b^2$ par 5.
2. Déterminer le reste dans la division euclidienne de 2025^{2025} par 7.

★★½☆☆ **Exercice 21** (Équation) .....

On considère l'équation dans $\mathbb{Z}$, $(E) : 2x^2 + 3y^2 = 16$.

1. Montrer que si un couple d'entiers (x, y) est solution de l'équation (E), alors $2x^2 \equiv 1[3]$.
2. Déterminer les restes dans la division euclidienne de $2x^2$ par 3. Et résoudre (E).

★★½☆☆ **Exercice 22** (Critères) .....

1. Déterminer les valeurs possibles du chiffre x pour que l'entier $\underline{71x4}_{10}$ soit divisible par 3.
2. Déterminer les valeurs possibles des chiffres x et y pour que l'entier $\underline{9x2y}_{10}$ soit divisible par 4.

★★★★☆ **Exercice 23** (Ordre) .....

Soient a et n deux entiers naturels.
On appelle **ordre de a modulo n** le plus petit entier naturel s, s'il existe, tel que

$$a^s \equiv 1[n].$$

1. On suppose qu'il existe m tel que $a^m \equiv 1[n]$.
   En utilisant la propriété de $\mathbb{N}$ qui dit que toute partie non vide de $\mathbb{N}$ admet un plus petit élément, prouver que s existe.
2. (a) En effectuant la division euclidienne de m par s, prouver que s divise m.
   (b) Montrer que quel que soit $n > 2$, $n - 1$ est d'ordre 2 modulo n.
3. **Application : $n = 7$**
   (a) Montrer que pour tout entier naturel a non multiple de 7, $a^6 \equiv 1[7]$.
   (b) Déterminer alors l'ordre de chacun des entiers non nuls strictement inférieurs à 7.

4. On pose $A_n = 1^n + 2^n + 3^n + 4^n + 5^n + 6^n$. Existe-t-il des valeurs de n pour lesquelles A_n est divisible par 7?

★★★½☆ **Exercice 24** (Suite #1)

On considère la suite $(u_n)_n$ d'entiers naturels définie par $\begin{cases} u_0 = 14 \\ u_{n+1} = 5u_n - 6, \text{ pour tout } n \in \mathbb{N} \end{cases}$

1. Calculer u_0, u_1, u_2, u_3 et u_4. Quelle conjecture peut-on émettre concernant les deux derniers chiffres de u_n?
2. Montrer que, pour tout $n \in \mathbb{N}$, $u_{n+2} \equiv u_n [4]$.
   En déduire que, pour tout $k \in \mathbb{N}$, $u_{2k} \equiv 2[4]$ et $u_{2k+1} \equiv 0[4]$.
3. Montrer que, pour tout $n \in \mathbb{N}$, $2u_n = 5^n + 2 + 3$.
   En déduire que, pour tout $n \in \mathbb{N}$, $2u_n \equiv 28[100]$.
4. Déterminer les deux derniers chiffres de l'écriture décimale de u_n suivant les valeurs de n.
5. Soit d un diviseur commun à tous les u_n. Montrer que $d = 1$ ou $d = 2$.

★★★½☆ **Exercice 25** (Suite #2)

On considère la suite $(u_n)_n$ d'entiers naturels définie par $\begin{cases} u_0 = 1 \\ u_{n+1} = 10u_n + 21, \text{ pour tout } n \in \mathbb{N} \end{cases}$

1. Calculer u_1, u_2 et u_3.
2. (a) Démontrer par récurrence que pour tout $n \in \mathbb{N}$, $3u_n = 10^{n+1} - 7$.
   (b) En déduire l'écriture décimale de u_n.
3. Démontrer que, pour tout entier naturel n, u_n n'est divisible ni par 2, ni par 3, ni par 5.
4. (a) Démontrer que pour tout $n \in \mathbb{N}$, $3u_n \equiv 4 - (-1)^n [11]$.
   (b) En déduire que, pour tout $n \in \mathbb{N}$, u_n n'est pas divisible par 11.
5. (a) Donner le reste de la division euclidienne de 10^4 par 17. En déduire que $10^{16} \equiv 1[17]$.
   (b) En déduire que, pour tout $k \in \mathbb{N}$, u_{16k+8} est divisible par 17.

★★★★☆ **Exercice 26** (Puissances)

On cherche à déterminer les couples (n, m) d'entiers naturels non nuls vérifiant la relation :

$$7^n - 3 \times 2^m = 1.$$

1. On suppose $m \leq 4$. Montrer qu'il y a exactement deux couples solutions.
2. On suppose maintenant que $m \geq 5$.
   (a) Montrer que si le couple (n, m) vérifie la relation précédente alors $7^n \equiv 1[32]$.
   (b) En étudiant les restes de la division par 32 des puissances de 7, montrer que si un couple (n, m) vérifie la relation, alors n est divisible par 4.
   (c) En déduire que si le couple (n, m) vérifie la relation alors $7^n \equiv 1[5]$.
   (d) Pour $m \geq 5$, existe-t-il des couples (n, m) d'entiers naturels vérifiant la relation?
   (e) Déterminer l'ensemble des couples (n, m) vérifiant la relation.

★★★★½ **Exercice 27** (Base 12)

Les chiffres en base 12 sont : $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \alpha, \beta$ (avec $\alpha = 10$, $\beta = 11$). Soit N d'écriture en base 12 :

$$N = \underline{a_n a_{n-1} \dots a_0}_{12} = a_n \times 12^n + a_{n-1} \times 12^{n-1} + \dots + a_0,$$

où $a_n, \dots, a_0$ sont des chiffres de la base 12.

1. (a) Démontrer que $N \equiv a_0 [3]$.
   (b) En déduire un critère de divisibilité par 3 pour un nombre écrit en base 12.
2. (a) Démontrer que $N \equiv a_n + \dots + a_0 [11]$.
   (b) En déduire un critère de divisibilité par 11 pour un nombre écrit en base 12.
3. Soit le nombre écrit en base 12 : $N = \underline{\beta 1 \alpha}_{12}$. Le nombre N est-il divisible par 3? par 11?