Chapitre 2

Divisibilité et congruences dans $\mathbb{Z}$

Dans ce chapitre nous allons nous focaliser sur les nombres entiers ($\mathbb{N}$ ou $\mathbb{Z}$) et nous allons nous intéresser aux propriétés satisfaites par de tels nombres.

2.1 Introduction

2.1.1 Survol historique

Cette branche des mathématiques est très ancienne et remonte à l'antiquité :

- au 3ième siècle avant *J.C.*, pour la première fois de l'Histoire, Euclide rassemble dans un livre (*les Eléments*) la majeure partie des connaissances des mathématiciens de l'époque. Parmi eux, il présente la définition de la division euclidienne (celle que vous avez rencontré en primaire).
- En -250, Diophante d'Alexandrie explique dans son ouvrage comment résoudre certaines équations dont les solutions sont des nombres entiers ou des fractions. En Chine, Sun Zi écrit lui aussi un traité de mathématiques et s'intéresse à des problèmes impliquant le reste d'une division euclidienne.
- Au 13ième siècle, les problèmes étudiés par Sun Zi sont complètement résolu par Qin Jiushao. Toutefois, son savoir ne dépasse pas les frontières chinoises avant le 20ième siècle.
- L'arithmétique est également très étudiée en Inde (Arybhata au 5ième siècle, Brahmagupta au 6ième siècle, Bhaskara au 12ième siècle,...).
- la civilisation islamique n'est pas reste également. Non seulement, elle véhicule le savoir acquis par les Grecs, Indiens et Chinois mais elle apporte des connaissances nouvelles Par exemple, Al-Kwarizmi écrit un livre sur la numération indienne.
- C'est à partir du 17ième siècle que l'Europe poursuit l'étude de cette branche de mathématique à partir d'une traduction en latin du livre de Diophante. Les questions soulevées intéressent alors les mathématiciens de l'époque (Fermat, Mersenne, Descartes,...) qui continuent d'explorer ce domaine. A ce moment là, Fermat annonça par missives à un collègue qu'il avait réussi à démontrer un théorème important (le *grand théorème de Fermat*) mais qu'il n'avait pas la place dans sa lettre pour développer sa démonstration. Nous ne serons jamais s'il avait

véritablement réussi mais il est certain qu'il fallut attendre les travaux d'Andrew Wiles en 1994 pour avoir une démonstration rigoureuse de l'affirmation de Fermat.

- Le 18ième siècle permet de voir briller les génies Euler, Legendre et Gauss dans ce domaine. D'ailleurs, Gauss démontra un théorème remarquable (appelée théorème de *réciprocité quadratique*) à l'âge de 17 ans. La théorie des nombres connait un essor sans pareil à cette période et les idées remarquables de Gauss furent enrichies par les travaux de Jacobi et Dirichlet.
- Même si nous ne poursuivons pas ce rapide survol historique, soyez certain que l'Histoire ne s'arrête pas ici et que, de nos jours, de nombreux mathématiciens continuent de chercher des solutions à des problèmes provenant de la théorie des nombres.

Bien que cela ne soit pas évident du tout, la théorie des nombres (et donc l'arithmétique) a donné naissance à la cryptographie : l'art de coder et décoder des messages. Par exemple, les protocoles de sécurité d'un site internet, d'une carte bancaire, de l'armée,... reposent sur des restes de divisions euclidiennes très compliquées. Bien entendu, ce résumé est un peu grossier et ne rend pas hommage aux travaux des mathématiciens *Rivest, Shamir et Adleman* qui ont crée le système de cryptage *R.S.A.*.

2.1.2 Problèmatique

Les objets que nous allons étudier permettent de résoudre le problème suivant.

Un satellite artificiel d'observation de la Terre a été placé sur une orbite parallèle à l'équateur à 12 000 km au dessus de la surface du globe. Nous considérons que sa trajectoire est un cercle dont le centre est celui de la Terre, que sa vitesse est constante et que sa période de révolution est de 7 heures.

Nous savons de plus que le 1er janvier 2020 à $0h00$, le satellite passe au-dessus de la Colombie et deux heures plus tard il survole le Kenya. De plus, le 8 janvier à $10h$, il se trouve au dessus de l'Indonésie.

1. Combien de fois le satellite survole-t-il la Colombie le 1er janvier 2020 ?
2. Donner les horaires de passages du satellite au-dessus du Kenya le 2 janvier.
3. Le satellite survolera-t-il le Kenya un jour à $0h00$?
4. Où se situe le satellite le 30 janiver à $6h00$ du matin ?
5. ...

2.2 Divisibilité dans $\mathbb{Z}$

2.2.1 Diviseurs et multiples

Rappelons que l'ensemble des entiers relatif $\mathbb{Z}$ est composé uniquement des entiers positifs et négatifs. L'ensemble des entiers naturel $\mathbb{N}$ est composé uniquement des entiers positifs.

Exemple 2.2.1. 1. $-2 \in \mathbb{Z}$ $10000 \in \mathbb{Z}$ mais $\sqrt{2} \notin \mathbb{Z}$ et $\frac{1}{3} \notin \mathbb{Z}$

2. $3 \in \mathbb{N}$ mais $3.15 \notin \mathbb{N}$, $-3 \notin \mathbb{N}$ et $\frac{3}{10} \notin \mathbb{N}$.

La première notion que nous allons étudier est celle de la divisibilité. Dans ce qui suit tout les nombres $a, b, c, k, \ldots \in \mathbb{Z}$

Définition 2.2.1. *Nous dirons qu'un nombre a divise un nombre b s'il existe un nombre $k \in \mathbb{Z}$ tel que*

$$b = ak$$

*et noterons ceci par $a|b$. Nous dirons alors que a est un **diviseur** de b ; de manière alternative, nous dirons que b est un **multiple** de a.*

Remarque.
1. Il n'est pas difficile d'observer que les nombres 1 et -1 divisent tous les entiers relatifs. En fait, ce sont les seuls éléments de $\mathbb{Z}$ vérifiant cette propriété. 0 est divisible par n'importe quel entier mais ne divise personne.
2. **Il est essentiel que** $k \in \mathbb{Z}$; dans ce chapitre à aucun moment $k \in \mathbb{R}$.
3. Si $n \in \mathbb{Z}^*$ alors tout diviseur de n est compris entre $-|n|$ et $|n|$. En particulier, tout entier relatif non nul admet un nombre fini de diviseur.
4. Soient $a, b \in \mathbb{Z}$ alors les propriétés suivantes sont équivalentes

$$a|b \iff -a|b \iff a|(-b) \iff -a|(-b).$$

Il va être important de se familiariser avec ces nouvelles notations et ce nouveau vocabulaire. Voyons quelques exemples.

Exemple 2.2.2.
1. $2|8$ car $8 = 2 \times k$ avec $k = 4 \in \mathbb{Z}$.
2. $6 \not| 21$ puisqu'il n'est pas possible de trouver $k \in \mathbb{Z}$ tel que $21 = 6k$.
3. -124 est bien un multiple de 4 car $4| - 124$. En effet, $-121 = 4 \times k$ avec $k = -31 \in \mathbb{Z}$.
4. 31 est diviseur de -124 puisque $121 = 31 \times k$ avec $k = -4 \in \mathbb{Z}$.

Exercices à traiter : 19,26 page 104.

Voici un nouveau raisonnement permettant de trouver les solutions **entières** d'une équation.

Exemple 2.2.3. Déterminons les solutions entières de (E) : $x^2 - y^2 = 7$.

1. (**Analyse**) Soit $(x; y)$ un couple de solution de (E), voyons quelles propriétés ce couple doit nécessairement vérifier.

$$x^2 - y^2 = 7 \iff (x - y)(x + y) = 7.$$

Nous constatons que $(x - y)$ et $(x + y)$ divisent le membre de gauche donc ce sont aussi des diviseurs du membre de droite. En outre, il facile de déterminer les diviseurs de 7, il s'agit de l'ensemble $\{-1; 1; 7; -7\}$. Nous devons donc résoudre les 4 systèmes d'équations envisageables :

$$\begin{cases} x + y = -7 \\ x - y = -1 \end{cases} \text{ ou } \begin{cases} x + y = -1 \\ x - y = -7 \end{cases} \text{ ou } \begin{cases} x + y = 1 \\ x - y = 7 \end{cases} \text{ ou } \begin{cases} x + y = 7 \\ x - y = 1 \end{cases}$$

Un simple calcul nous mène à

$$\left\{\begin{array}{l} 2x=-8 \\ x-y=-1 \end{array}\right. \quad \text{ou} \quad \left\{\begin{array}{l} 2x=-8 \\ x-y=-7 \end{array}\right. \quad \text{ou} \quad \left\{\begin{array}{l} 2x=8 \\ x-y=7 \end{array}\right. \quad \text{ou} \quad \left\{\begin{array}{l} 2x=-8 \\ x-y=1 \end{array}\right.$$

Les candidats potentiels sont donc $(x;y)=(-4;-3)$ ou $(x;y)=(-4;3)$ ou $(x;y)=(4;-3)$ ou $(x;y)=(4;3)$.

2. (**Synthèse**) Il ne reste plus qu'à regarder si les couples obtenus sont bien solutions de (E). Ici, c'est bien le cas.
3. (**Conclusion**) L'ensemble des solutions de (E) est $\big\{(-4;-3)\,;\,(-4;3)\,;\,(4;-3)\,;\,(4;3)\big\}$.

Remarque. Le raisonnement précédant est un procédé **d'analyse/synthèse**. D'abord, nous supposons que les solutions de problèmes existent et cherchons à obtenir une liste réduite de candidats. Ensuite, nous regardons parmi ces candidats lesquels sont solutions pour enfin conclure.

Exercices à traiter : 29 et 35 page 104.

Essayons maintenant de voir comment se comporte la propriété de division.

Proposition 5 (Transitivité de la divisiblité)**.** *Soient $a,b,c\in\mathbb{Z}$. Si $a|b$ et $b|c$ alors $a|c$.*

Démonstration. (L'idée de la preuve est à retenir)

1. But : nous voulons montrer que $a|c$. Autrement dit, il faut trouver $K\in\mathbb{Z}$ tel que $c=aK$.
2. Par définition, puisque $a|b$ il existe $k\in\mathbb{Z}$ tel $b=ak$. De même, il existe $k'\in\mathbb{Z}$ tel que $c=bk'$ (a priori k est différent de k'). Par suite,

$$c=bk'=(ak)k'=akk'=aK \quad \text{en posant} \quad K=kk'\in\mathbb{Z}$$

donc $a|c$.

□

Remarque. La propriété de transitivité est à rapprocher de celle plus connue des droites parallèles : si $d_1//d_2$ et $d_2//d_3$ alors $d_1//d_3$.

Voyons ce que nous pouvons obtenir d'autre.

Proposition 6 (Divisibilité et combinaison linéaire)**.** *Soient $a,b,c\in\mathbb{Z}$.*

1. si $a|b$ et $a|c$ alors

$$a|(kb+lc) \quad \textit{pour n'importe quel choix d'entiers} \quad k,l\in\mathbb{Z}$$

2. En particulier, si $a|b$ alors

$$a|(a+b) \quad \textit{et} \quad a|a-b/$$

Remarque. La quantité $kb+lc$ s'appelle une **combinaison linéaire** de a et b.

Démonstration. 1. **Exercice à traiter :** exercez-vous à la démonstration en établissant le premier item. *Indication : s'inspirer de la démonstration de la proposition précédente.*

2. Le deuxième point s'obtient en choisissant des valeurs particulières de c, k et l. Par exemple, si $c = a$, $k = l = 1$, nous avons

$$a|b \quad \text{et} \quad a|a \quad \text{donc} \quad a|(1 \times a + 1 \times b) = a + b.$$

□

Voyons comment utiliser cette propriété pour résoudre le problème suivant.

Exemple 2.2.4. Déterminer tous les entiers $n \in \mathbb{Z}$ tels que $(2n + 7)|(n - 3)$.

Pour cela, il convient de trouver une combinaison linéaire de $a = 2n + 7$ et de $b = n - 3$ ne faisant pas intervenir n. Par exemple, si $k = 1$ et $l = -2$ nous trouvons

$$ka + lc = 2n + 7 - 2(n - 3) = 13. \tag{2.2.1}$$

1. Nous pouvons débuter notre **analyse**. Soit $n \in \mathbb{Z}$ tel que $(2n + 7)|(n - 3)$. Remarquons que

$$(2n + 7)|(2n + 7) \quad \text{et} \quad (2n + 7)|(n - 3).$$

D'après la proposition 6, nous savons donc que $(2n + 7)$ divise n'importe quelle combinaison linéaire de $(2n+7)$ et de $(n-3)$. C'est en particulier vrai pour la combinaison linéaire (2.2.1). Autrement dit

$$2n + 7|2n + 7 - 2(n - 3) = 13$$

Il ne reste plus qu'à lister les diviseurs de 13 puisque $2n + 7$ en fait forcément parti. Puisque $-1, 1, 13$ et -13 sont les seuls diviseurs de 13, nous devons résoudre

$$2n + 7 = -1 \quad \text{ou} \quad 2n + 7 = -13 \quad \text{ou} \quad 2n + 7 = 1 \quad \text{ou} \quad 2n + 7 = 13.$$

Il y a donc 4 possibilités $-4, -10, -3$ et 3.

2. Faisons la **synthèse** et regardons parmi nos **candidats** lesquels sont solutions. Par exemple, si $n = -4$ alors $2n + 7 = -1$ et $n - 3 = -7$ or $-1| - 7$ donc -4 est une solution. En procédant de mêmes avec les autres, nous constatons qu'il s'agit à chaque fois d'une solution.

Exercices à traiter : 31,32,33 page 104.

2.3 Division euclidienne

Procédons à un rappel de primaire en effectuant la division euclidienne de 23 par 4

$$\begin{array}{r|l} 2\ 3 & 4 \\ \hline 3 & 5 \end{array}$$

Nous savons donc que $23 = 4 \times 5 + 3$: $a = 23$ est le **dividende**, $b = 4$ est le **diviseur**, $q = 5$ est le **quotient** et $r = 3$ est le **reste** ; il est essentiel que $0 \leq r < b$, autrement, nous pourrions poursuivre la division. Observons en passant que $\frac{23}{4} = 5,75$, il n'est donc pas possible d'ôter plus de 5 fois 4 de 23 (5 est la partie entière de $\frac{23}{4} = 5,75$) ; le reste s'obtient ensuite en effectuant le calcul suivant $r = 23 - 4 \times 5$.

Voyons comment formaliser cette observation.

Théorème 7 (Division euclidienne)**.** *Soient $a, b \in \mathbb{N}$ avec $b \neq 0$. Alors il existe un* ***unique couple d'entiers*** *naturel $(q; r)$ satisfaisant les conditions suivantes :*

1. *$a = bq + r$.*
2. *le reste est* ***strictement plus petit*** *que le diviseur b : $0 \leq r < b$.*

Remarque.
1. Ceci peut s'étendre facilement à $\mathbb{Z}$. Dans ce cas, il faut modifier légèrement l'énoncé : $q \in \mathbb{Z}$, $r \in \mathbb{N}$ et le reste vérifie $0 \leq r < |b|$.
2. Observons également le fait suivant : puisque le reste est un entier $0 \leq r < b$, forcément $r \in \{0\,;\,1\,;\,2\,;\,\ldots\,;\,b-1\}$. Par exemple, le reste de la division par 2 est forcément 0 ou 1 ; celui de la division par 3 est forcément 0 ou 1 ou 2.

Démonstration. Pour démontrer cela, il suffit de reprendre ce que nous avons fait pour diviser 23 par 4.

1. En guise de préambule, il faut rappeler la notion de partie entière $\lfloor x \rfloor \in \mathbb{N}$ d'un nombre $x \in \mathbb{R}$. Ce nombre vérifie
$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$
Voyons quelques exemples pour s'en convaincre $\lfloor 2,999 \rfloor = 2$, $\lfloor -4 \rfloor = -4$ et $\lfloor \pi \rfloor = 3$. Observons au passage que si $x \geq 0$ alors $\lfloor x \rfloor \geq 0$.
2. (Existence). Nous allons montrer que le couple $(q; r)$ existe et vérifie les propriétés voulues. Tout d'abord, nous devons savoir combien de fois au maximum, il est possible d'ôter b de a. Cela revient à considérer $\lfloor \frac{a}{b} \rfloor$; notons ce nombre $q \in \mathbb{N}$. Par définition de la partie entière, nous savons que
$$q \leq \frac{a}{b} < q + 1 \quad \Longleftrightarrow \quad bq \leq a \leq b(q+1) \quad \text{puisque} \quad b > 0.$$
En soustrayant bq à chaque membre de cette inégalité, nous obtenons
$$0 \leq a - bq < b$$
et nous savons qu'il n'est plus possible de soustraire b à nouveau (à cause de l'inégalité stricte). Il parait alors naturel de poser
$$r = a - bq.$$
Nous avons donc obtenu un couple d'entiers (q, r) tel que $a = bq + r$ et $0 \leq r < b$.
3. (Unicité). Supposons qu'il existe deux couples d'entiers (q, r) et (q', r') tels que
$$a = bq + r \quad \text{avec} \quad 0 \leq r < b \quad \text{et} \quad a = bq' + r' \quad \text{avec} \quad 0 \leq r' < b.$$
En particulier, nous avons
$$bq + r = b'q + r' \quad \Longleftrightarrow \quad b(q - q') = r' - r.$$
La dernière égalité signifie que $r' - r$ est un multiple de b. Nous allons montrer que ce multiple est forcément 0. Nous savons que
   - $0 \leq r < b \quad \Longleftrightarrow -b < -r \leq 0$,
   - $0 \leq r' < b$.

Donc, en additionnant ces deux inégalités, nous en déduisons que que $-b < r' - r < b$. Or le seul multiple de b compris strictement entre $-b$ et b est 0. Cela signifie que

$$r' - r = 0 \quad \Longleftrightarrow \quad r = r'.$$

Par suite, $bq + r = bq' + r' \quad \Longleftrightarrow \quad bq = bq' \quad \Longleftrightarrow \quad q = q'$. Autrement dit les couples (q, r) et (q', r') sont identiques.

□

Il est impératif de savoir poser une division euclidienne et la manipuler.

Exemple 2.3.1. 1. Si $a = 80$ et $b = 17$ alors

$$80 = 17 \times 4 + 12 \quad \text{et} \quad 0 \leq 12 < 17 \quad \text{donc} \quad q = 4 \quad \text{et} \quad r = 12.$$

2. Dans la division de -37 par $b \in \mathbb{N}^*$, le reste est 14. Quelles sont les valeurs possible du diviseur b et du quotient q ?

   Forcément, nous avons $-37 = qb + 14$ avec $14 < b$. Ceci mène à

   $$qb = -51$$

   Il ne reste plus qu'à étudier les diviseurs de -51. Il s'agit de $-51, -17, -3, -1, 1, 3, 17, 51$. Puisque $b > 14$ forcement $b = 17$ (d'où $q = -3$) ou $b = 51$ d'où $(q = -1)$.

Par la suite, il sera important de raisonner en fonction des restes envisageables.

Exemple 2.3.2. Soit $n \in \mathbb{N}$, montrons que $A = n(n^2 + 5)$ est divisible par 3. Il faut procéder par disjonction de cas :

1. Si $n = 3k$ (i.e. le reste après la division de n par 3 est nul) alors

   $$A = 3k(9k^2 + 5) = 3K_1 \quad \text{avec} \quad K_1 = k(9k^2 + 5) \in \mathbb{Z}.$$

2. Si $n = 3k + 1$ (i.e. le reste vaut 1 après la division de n par 3) alors

   $$A = (3k+1)(9k^2+6k+6) = 3(3k+1)(3k^2+2k+2) = 3K_2 \quad \text{avec} \quad K_2 = (3k+1)(3k^2+2k+2) \in \mathbb{Z}.$$

3. Si $n = 3k + 2$ (i.e. le reste vaut 2 après la division de n par 3) alors

   $$A = (3k+2)(9k^2+12k+9) = 3(3k+2)(3k^2+4k+3) = 3K_3 \quad \text{avec} \quad K_3 = (3k+2)(3k^2+4k+3) \in \mathbb{Z}.$$

A chaque fois nous avons montré que A était divisible par 3. Puisque que nous avons énuméré toutes les possibilité, A est bien divisible par 3 pour tout $n \in \mathbb{N}$.

Exercices à traiter : 79 (Q1 et Q2) page 107 ; 45 page 105 ; 80 page 107, 82 page 108 ; 39,41 page 105 et 86 page 108.

2.4 Congruences

Nous allons voir que la division euclidienne permet d'obtenir de nombreuses informations utiles. En particulier, nous allons voir qu'il suffit de se concentrer sur la valeur du reste.

2.4.1 Définition

Définition 2.4.1. *Soient $a, b \in \mathbb{Z}$ et $n \geq 2$ un entier naturel. Nous dirons que a est congru à b modulo n si a et b ont le même reste dans division euclidienne par n. Nous noterons ceci par*

$$a \equiv b[n] \quad ou \quad a \equiv b \bmod n$$

Remarque. En particulier, $a \equiv b[n]$ est équivalent à dire que $a - b$ est un multiple de n : il existe donc $k \in \mathbb{Z}$ tel que

$$a - b = kn.$$

Cette propriété est très utile en pratique.

Voyons sur quelques exemples.

Exemple 2.4.1.
1. $-5 \equiv 3[2]$ car -5 et 2 ont pour reste 1 dans la division euclidienne par 2.
2. $4 \equiv 0[4]$ et $8 \equiv 0[4]$.

Voyons à présent quelques conséquences de cette nouvelle définition.

Proposition 8. *Soient $a, b, c \in \mathbb{Z}$ et $n \geq 2$ un entier naturel.*

1. *(Réfléxivité) $a \equiv a[n]$.*
2. *(Symétrie) $a \equiv b[n]$ si et seulement si $b \equiv a[n]$.*
3. *(Transitivité) si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$.*
4. *(Calcul pratique) Si r est le reste de la division euclidienne de a par n alors $a \equiv r[n]$. En particulier,*

$$a \quad \textit{est divisible par} \quad n \quad \Longleftrightarrow \quad a \equiv 0[n].$$

Exercices à traiter : 46 page 105, 92 et 95p209, 97 (Q2 et Q4) p109

2.4.2 Congruences et opérations

Il est important de voir comment les opérations usuelles se comportent avec les congruences. Est-il possible d'additionner ou multiplier des congruences ?

Proposition 9. *Soient $a, b, c, d \in \mathbb{Z}$ et $n \geq 2$ un entier naturel. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors*

1. *$a + c \equiv b + d[n]$*
2. *$a - b \equiv b - d[n]$*
3. *$ac \equiv bd[n]$. En particulier, pour tout $p \geq 1$ nous avons $a^p \equiv b^p[n]$.*

Remarque. Attention le cas de la division est beaucoup plus délicat et ne s'énonce pas aussi simplement. Cet aspect sera abordé ultérieurement.

Démonstration. Il est important de saisir le mécanisme des démonstrations, celui-ci sera utile dans certains exercices. Traitons le premier point, les autres sont laissés à titre d'exercice.

- Tout d'abord, il faut revenir à la définition : $a \equiv b[n]$ et $c \equiv d[n]$, signifie qu'il existe des entiers $k, k' \in \mathbb{Z}$ tel que

$$a - b = kn \quad \text{et} \quad c - d = k'n$$

- Il faut ensuite voir ce que nous souhaitons obtenir : $a+c \equiv b+d[n]$ signifie qu'il existe $K \in \mathbb{Z}$ tel que

$$(a+c) - (b+d) = Kn \quad (\text{autrement dit : } \quad (a+c) - (b+d) \quad \text{est un multiple de } \quad n).$$

- Il ne reste plus qu'à déterminer $K \in \mathbb{Z}$ à partir de nos hypothèses :

$$(a+c) - (b+d) = (a-b) + (c-d) = kn + k'n = (k+k')n = Kn$$

avec $K = k + k' \in \mathbb{Z}$.

□

Voyons à présent deux applications de ces nouvelles notions.

Exemple 2.4.2. Montrer que, pour tout entier $n \in \mathbb{Z}$, $n(n+1)(2n+1)$ est divisible par 3. Pour cela, il suffit de dresser un tableau de congruences de n modulo 3 et d'utiliser les règles décrites plus haut. Rappelons au passage que les restes de la division de n par 3 ne peuvent être que $0, 1$ ou 2. Pour alléger les notations nous utiliserons la notation $P = n(n+1)(2n+1)$.

$n \equiv \ldots [3]$	0	1	2
$(n+1) \equiv \ldots [3]$	1	2	$3 \equiv 0$
$(2n+1) \equiv \ldots [3]$	1	$3 \equiv 0$	$5 \equiv 2$
$P \equiv \ldots [3]$	$0 \times 1 \times 1 \equiv 0$	$1 \times 2 \times 0 \equiv 0$	$2 \times 0 \equiv 2 \equiv 0$

Dans tous les cas, nous avons montrer que $P \equiv 0[3]$. Autrement dit P est divisible par 3.

Exercices à traiter : 51,53 page 105

Exemple 2.4.3. Quel est le reste de la division euclidienne de 23^{137} par 7 ?

- Tout d'abord il convient de déterminer (si elle existe) une puissance $n > 0$ (la plus petite possible) telle que $23^n \equiv 1[7]$ afin de simplifier nos calculs.

$$23^0 = 1 \quad \text{donc} \quad 23^0 \equiv 1[7], \quad 23^1 = 23 = 3 \times 7 + 2 \quad \text{donc} \quad 23^1 \equiv 2[7]$$
$$23^2 \equiv 23 \times 2 \equiv 4[7] \quad \text{et} \quad 23^3 \equiv 23 \times 4 \equiv 92 \equiv 1[7]$$

puisque $92 = 13 \times 7 + 1$. La puissance recherchée vaut donc $n = 3$.
- Il reste maintenant à diviser 137 par 3, il vient

$$137 = 45 \times 3 + 2$$

Ainsi,

$$23^{137} \equiv 23^{3\times 45+2} \equiv (23^3)^{45} \times 23^2 \equiv 1^{45} \times 4 \equiv 4[7].$$

Remarque. 1. Nous avons montré que $23^3 \equiv 23 \times 23^2 \equiv 1[7]$. Autrement dit, l'inverse de 23 modulo 7 vaut 23^2. De manière général, étant donné $a \in \mathbb{Z}$ et $n \geq 2$ un entier, nous dirons que b est l'inverse de a modulo n si

$$ab \equiv 1[n].$$

Par exemple, 8 est l'inverse de 2 modulo 3 puisque $8 \times 2 \equiv 16 \equiv 1[3]$.

2. Le reste de la division euclidienne de 23^{137} par 7 vaut donc 4. Bien entendu, la possibilité de déterminer l'inverse b d'un nombre a modulo n dépend du nombre n. Si $n = 4$, il n'est pas possible de trouver d'inverse au nombre $a = 8$ puisque

$$8 \equiv 0[4].$$

Observons également le fait curieux suivant

$$2 \times 4 \equiv 0[4].$$

Autrement dit, le produit de deux nombres **non nuls** a et b donne un résultat **nul** ; ceci n'était pas envisageable lorsque nous manipulions des nombres réels ou complexes (règle du produit nul). *Challenge : proposer un autre ensemble (de nombres, de fonctions, ...) dans lequel ce genre de phénomène se produit*.

Exercices à traiter : 52p105, 99p109, 103p110, 110p110, 116p111, 109p111.

2.5 Pour aller plus loin : relations d'équivalences

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

Exemple 2.5.1. Modulo 2, les nombres entiers sont regroupés en deux ensembles disjoints :

$$\text{les nombres pairs : } 0\,;\,2\,;\,4\,;\,\ldots \quad \text{et les nombres impairs : } \quad 1\,;3\,;\,5\,;\,\ldots$$

Le premier de ces ensembles regroupent tout les nombres $n \in \mathbb{Z}$ dont le reste dans la division euclidienne par 2 vaut 0, tandis que le second est composé des éléments dont le reste vaut 1 ; notons ces ensembles respectivement [0] et [1].

En pratique, modulo 2, nous ne faisons aucune différence entre les nombres 0, 2, 4, -2,... ou les nombres -1, 1, 3, ... Pour simplifier les calculs nous travaillons plutôt avec l'un d'entre eux (le plus simple) qui fait office de **représentant**. C'est-à-dire :

$$[0] \quad \text{représente } \textbf{tous} \text{ les nombres pairs} \quad \text{et} \quad [1] \quad \text{représente } \textbf{tous} \text{ les nombres impairs.}$$

Par la suite, pour alléger les notations, les crochets ne sont pas forcément indiqués dans les calculs car cela permet de traiter les manipulations algébriques de manière plus naturelle (« comme avant (avec des réels) »).

1. Implicitement ce genre de chose a déjà été entrevu avec les fractions :

$$\frac{1}{2} = \frac{2}{4} = \frac{-4}{-8} = \dots$$

Cette fois-ci nous identifions une fraction $\frac{a}{b}$ avec une fraction $\frac{c}{d}$ lorsque

$$ad = bc.$$

2. Il serait possible d'imaginer des situations similaires hors d'un contexte mathématique. Par exemple, en décidant qu'un habitant d'une agglomération est choisi pour représenter sa commune (il faut alors supposer que le lieu de résidence est unique). Concernant Lille (la métropole lilloise au sens large), il sera alors équivalent d'utiliser

Mme Aubry $\sim$ l'enseignant de mathématiques $\sim$ un élève de terminale option maths expertes

pour représenter la commune.

Formellement, ce procédé d'identification porte le nom de **relation d'équivalence**. Grossièrement, il s'agit d'établir une règle $\mathcal{R}$ permettant de savoir si deux éléments d'un ensemble (non vide) E vérifient la même propriété ; nous dirons que de tels éléments sont équivalents.

Définition 2.5.1. *Soit E un ensemble non vide, nous dirons que $\mathcal{R}$ est une relation d'équivalence sur $E \times E$ lorsque $\mathcal{R}$ vérifie les propriétés suivantes*

1. *(réflexivité) pour tout $x \in E$, $x\mathcal{R}x$.*
2. *(symétrie) soient $x, y \in E$ alors $x\mathcal{R}y \iff y\mathcal{R}x$.*
3. *(transitivité) soient $x, y, z \in E$, si $x\mathcal{R}y$ et $x\mathcal{R}z$ alors $x\mathcal{R}z$.*

Remarque. Dans le cours nous avons montré que la relation de congruence $\equiv$ était une relation d'équivalence :

$$x\mathcal{R}y \quad \iff \quad a \equiv b[n] \quad \iff \quad a - b \quad \text{est un multiple de n.}$$

Etant donné une relation d'équivalence, il est possible de regrouper les éléments de E par paquets disjoints.

Définition 2.5.2. *Soit E un ensemble non vide, muni d'une relation d'équivalence $\mathcal{R}$. Soit $x \in E$, la classe d'équivalence $[x]$ associée à x est composée de tous les éléments de E en relation avec x. Autrement dit,*

$$[x] = \big\{ y \in E \quad ; \quad x\mathcal{R}y \big\}.$$

*Nous dirons que $[x]$ est **un représentant** de la classe d'équivalence.*

Remarque.
1. Une classe d'équivalence ne dépend pas du choix de son représentant et l'ensemble des classes d'équivalences forme une partition de E.
2. Lorsque $E = \mathbb{Z}$ et $\mathcal{R}$ est la relation de congruence modulo n, les classes d'équivalences sont données par les différents restes possibles de la division euclidienne de a par n. Si $n = 2$, il n'y a que deux classes d'équivalences :

$$[0] = \{\dots ; -2 ; 0 ; 2 ; 4 ; \dots\} \quad \text{et} \quad [1] = \{\dots ; -1 ; 1 ; 3 ; 5 ; \dots\}.$$

3. Sans entrer dans les détails, à partir d'un ensemble E muni d'une relation d'équivalence $\mathcal{R}$, il est possible de parler d'unicité « à la relation d'équivalence près ». Cela mène à la notion *d'ensembles quotients*. C'est d'ailleurs pour cela que l'ensemble des restes (parfois appelés résidus) d'une division euclidienne par n est noté $\mathbb{Z}/n\mathbb{Z}$.